2

ISSN: 2955-0270
eISSN: 3028-3310

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

Revista Ciberespacio, Tecnología e Innovación

Volumen 1 - Número 2
2022 (julio-diciembre)
Bogotá., Colombia

Revista **Ciberespacio, Tecnología e Innovación**

Volumen 1, número 2, julio-diciembre 2022
ISSN: 2955-0270 • eISSN: 3028-3310
Bogotá, D.C., Colombia

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 1, número 2, julio-diciembre 2022
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**.

2022, 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

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 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

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 icono 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

Esta página queda intencionalmente en blanco

Editorial

Editorial

Esta página queda intencionalmente en blanco

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 1, número 2, julio-diciembre 2022 (pp. 111-112)
Bogotá, D.C, Colombia

EDITORIAL **ESDEG**

Editorial: Retos y desafíos en el ciberespacio para Colombia

Editorial: Challenges in cyberspace for Colombia

DOI: https://doi.org/10.25062/2955-0270.4802

Tania Lucia Fonseca Ortiz
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

La Revista Ciberespacio, Tecnología e Innovación (RCIT) tiene como objetivo visibilizar los resultados de investigación mediante la publicación académica. Para finalizar el año, y bajo los objetivos estratégicos establecidos de Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG), considerada la institución principal del Comando General de las Fuerzas Militares de Colombia, se buscó abrir el debate y despertar el interés del ciberespacio en el entorno militar a nivel estratégico. Por lo anterior, en el volumen 1 del número 2, abre el debate sobre los *retos y desafíos en el ciberespacio en Colombia*.

Para *Sección Debates* se presentan tres resultados de investigación enfocados a diferentes campos. El primero, t*itulado Modelo de ciberseguridad aplicable en el comercio marítimo en Colombia para contener amenazas del ciberespacio*, propone un modelo de ciberseguridad que es aplicable al campo marítimo. En este artículo se analiza la importancia de proteger a la infraestructura marítima contra amenazas provenientes del ciberespacio, considerando que existen riesgos y peligros que pueden atentar ante infraestructuras críticas importantes para el desarrollo del Estado colombiano. El escrito finaliza con una propuesta de modelo de ciberseguridad donde se establezca el rol de la Armada Nacional de Colombia para promover la prevención de incidentes, una interesante investigación que demuestra la importancia del poder marítimo para la nación.

El segundo, *El ciberespacio como variable habilitante para la movilización de masas y desestabilización del orden público en Colombia*, realiza un análisis enfocado a la movilización social, un fenómeno que afectó a Colombia y que fue impulsado mediante el empleo de canales de información y comunicación en el ciberespacio. Tomando ejemplos de caso, se despierta la importancia de comprender el ciberespacio como una variable que puede afectar el orden público, pero al mismo tiempo, se afirma que oportunidad para que los tomadores de decisiones reconozcan dicho medio como una herramienta de las nuevas generaciones para comunicarse y comprender las demandas sociales.

Tercero, *El Ciberespacio como escenario para enfrentar los delitos transnacionales en Colombia*, es un artículo de debate que resalta las implicaciones del uso de tecnologías por parte de actores irregulares. Se señala que la globalización generó una trasformación en las relaciones sociales que también afecto a las organizaciones, puntualizado, que el crimen organizado también se está aprovechando de un nuevo escenario, es por esto, que debe considerarse un dominio que puede potencializar la lucha contra diferentes delitos que requiere conectividad, accesos oportunos y efectivos a la información.

Cuatro, en la *Sección Coyuntura,* se resalta el análisis sobre *La regulación del ciberespacio como principal ecosistema de la cuarta revolución industrial*. En este escrito se resalta la importancia de las revoluciones tecnológicas, señalando que las cuarta abrió nuevas regulaciones para Colombia.

Quinto, en la *Sección Perspectivas,* se realiza la entrevista a Steven Jones-Chaljub, un referente académico e intelectual. Como tema de discusión se propuso *El ciberespacio humano: retos y perspectivas*, señalando los efectos del ciberespacio en las relaciones cotidianas y efectos que se están identificando.

Sexto, en la *Sección Enfoques*, se realiza una recomendación para la lectura del libro desarrollado por La ciberseguridad, sus impactos y desafíos, el Centro de Estudios Estratégicos (CEEAG) de Chile, un centro de investigación que se encuentra desarrollando proyectos de investigación relacionados con la ciberguerra. En este escrito se resaltan los avances en temas conceptuales y del ámbito militar en Chile.

Finalmente, se invita a la comunidad académica, científica y de expertos, a compartir este número y, al mismo tiempo, invitarlos a participar para que publiquen sus resultados de investigación, perspectivas o recomendaciones en este medio de difusión y, de esta manera, despertar el interés sobre el ciberespacio, la tecnología y la innovación.

Debates

Debates

Esta página queda intencionalmente en blanco

Revista Ciberespacio, Tecnología e Innovación
Volumen 1, número 2, julio-diciembre 2022 (pp. 115-143)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Modelo de ciberseguridad aplicable en el comercio marítimo en Colombia para contener amenazas del ciberespacio

Cybersecurity model applicable in maritime commerce in Colombia to contain cyberspace threats

DOI:https://doi.org/10.25062/2955-0270.4771

Juan Pablo Gómez López

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

Resumen

El objetivo de proponer un modelo conceptual de ciberseguridad aplicable en el comercio marítimo en Colombia, por eso tiene un enfoque cualitativo aplicado por medio de instrumentos de investigación como la revisión documental en fuentes primarias que incluyen libros, informes, páginas web, crónicas, noticias; el segundo instrumento son entrevistas a personal que trabaja en áreas relacionadas con la ciberseguridad en la Armada Nacional, a partir de esta información, de la que se obtiene de documentos y de casos en otros países se elabora un modelo de ciberseguridad aplicable en el comercio marítimo en Colombia para contener amenazas del ciberespacio que cuenta con tres componentes enfocados en la prevención y minimización de delitos como el narcotráfico y la piratería que están relacionados con este fenómeno a través de la contribución de la Armada; el modelo propuesto es verificado por expertos en el tema y contrastado a través de una matriz DOFA.

Palabras Clave: Armada Nacional, Ciberamenazas, Ciberseguridad, Comercio Marítimo

Abstract

The objective of proposing a conceptual model of cybersecurity applicable to maritime commerce in Colombia, for this reason it has a qualitative approach applied through research instruments such as documentary review in primary sources that include books, reports, pages web, chronicles, news; The second instrument is interviews with personnel who work in areas related to cybersecurity in the National Navy. Based on this information, which is obtained from documents and cases in other countries, a cybersecurity model applicable to maritime trade is developed. in Colombia to contain threats from cyberspace, which has three components focused on the prevention and minimization of crimes such as drug trafficking and piracy that are related to this phenomenon through the contribution of the Navy; the proposed model is verified by experts in the field and contrasted through a SWOT matrix.

Key words: National Navy, Cyberthreats, Cybersecurity, Maritime Trade

Artículo de Debates
Recibido: 18 de agostode 2022 • **Aceptado:** 14 de diciembre de 2022
Contacto: Juan Pablo Gómez López gomezlj@esdeg.edu.co

Introducción

La globalización es uno de los fenómenos que cambio la dinámica del mundo haciendo posible la materialización de una sociedad interconectada a través de internet y otros sistemas de comunicación, así mismo, fue el punto de partida para el desarrollo de herramientas que han simplificado procesos logísticos en sectores como el comercio marítimo, en donde internet se complementa con el ciberespacio para ayudar en la digitalización de sistemas de navegación, radares y la implementación de otros instrumentos que mejoran la gestión y la seguridad de buques y barcos que transportan mercancía por el mundo. Pero, lo que en un momento se reconoció como una ventaja, con el paso del tiempo ha expuesto también amenazas que a través del ciberespacio han afectado el funcionamiento y la seguridad del comercio marítimo en Colombia.

Entre tanto, el ciberespacio, reconocido como un mundo virtual en el que interactúan diferentes actores a través de herramientas tecnológicas en donde se forja un espacio relacional (Aguirre, 2010), influye en la evolución de la sociedad, pero con el paso de los años este se ha transformado en una amenaza para actividades como el comercio marítimo, víctima de ataques que evidencian la vulnerabilidad de la seguridad marítima y cibernética, afectándolo con la irrupción de sistemas marítimos que se suman a la llegada de intrusos y de virus que, a su vez, exponen amenazas de otra naturaleza que pueden entorpecer el correcto funcionamiento de instituciones estatales.

El auge del ciberespacio, la aparición de herramientas que afectan el comercio marítimo y otros aspectos del mundo globalizado expone que las amenazas del ciberespacio son el resultado del avance tecnológico y de la inminente necesidad que tienen las personas por utilizar internet en su vida diaria y, en otros aspectos, como el desarrollo de las economías y sociedades, pero, cuando esta tecnología es utilizada para intervenir bases de datos, sistemas y softwares de seguridad es posible afectar a través de la intrusión de redes que funcionan con la tecnología de la *big data* la actividad económica marítima del mundo y, por ende, de Colombia.

Esta problemática no es ajena al escenario colombiano, por eso, Grimalt y Baró (2021), muestran la manera como la ciberdelincuencia se posiciona en el contexto nacional por medio de la interceptación de los sistemas de seguridad de la actividad portuaria y marítima, razón por la que se han creado estrategias para hacer frente a flagelos como el narcotráfico, la migración ilegal, el hurto, entre otros delitos relacionados con archivos maliciosos para acceder a sistemas y datos importantes, la interferencia en los sistemas de identificación de los barcos, del seguimiento de las cargas a través de GPS y el impedimento para visualizar las cartas electrónicas (Grimalt y Baró, 2021).

El contexto actual de la problemática de las amenazas provenientes del ciberespacio en el comercio marítimo y la justificación que demuestra la necesidad de estudiar el

problema es explicada por la Armada Nacional en el Plan Estratégico Naval (2015), documento en donde la Institución expone que las amenazas cibernéticas a la seguridad de la actividad marítima crecen constantemente, por eso se hace necesaria la búsqueda de modelos con los que desde su misión esperan intervenir el ciberespacio para neutralizar los ataques informáticos, defender los intereses marítimos y fluviales de Colombia, haciendo uso del desarrollo del poder militar y naval que es representado por la Armada Nacional.

En tal sentido, al identificar las amenazas que puedan afectar el comercio marítimo de un país, se estipula como pregunta de investigación: ¿Cuál debe ser el modelo de ciberseguridad aplicable en el comercio marítimo en Colombia para la contención de amenazas provenientes del ciberespacio?, mediante un análisis documental y fuentes de información que lleven a identificar modelos que permitan contrarrestar dichas amenazas.

Por consiguiente, como tesis central se establece un modelo de ciberseguridad aplicable en el comercio marítimo en Colombia para la contención de amenazas provenientes del ciberespacio, permitiendo desde el poder militar y naval que representa la Armada Nacional, intervenir todas las estrategias que afecten esta actividad económica marítima y los intereses de la Nación.

Finalmente, la metodología implementada en el desarrollo de la investigación es enfoque cualitativo con una orientación interpretativa, razón por la que se recolecta información que posteriormente se clasifica a través del método de la triangulación hermenéutica para, luego, analizar los datos recolectados con el fin de dar respuesta al interrogante formulado como pregunta de investigación (Hernández, Fernández y Baptista, 2014).

Metodología

El alcance la investigación consiste en proponer un modelo conceptual de ciberseguridad para el comercio marítimo en Colombia. Para su desarrollo se establecieron tres objetivos específicos que se desarrollaron en tres fases respectivamente.

La primera consistió en caracterizar las amenazas cibernéticas que afectan la seguridad de la información del comercio marítimo colombiano por medio de la revisión documental de fuentes primarias y secundarias, tanto en primera y segunda fase, que incluyen informes, artículos, trabajos de investigación y normatividad vigente. Estas fueron revisadas y analizadas por medio del método de triangulación hermenéutica, con el propósito de identificar dichas amenazas.

Asimismo, la aplicación de entrevistas como instrumento de investigación al personal relacionado con la actividad en el mar, teniendo en cuenta variables como:

Ciberseguridad en el comercio marítimo, comercio marítimo y amenazas del ciberespacio al comercio marítimo, arrojando como resultado una matriz de caracterización de amenazas cibernéticas y las necesidades de ciberseguridad para el comercio marítimo colombiano.

Posteriormente, la segunda fase permite definir un modelo conceptual de ciberseguridad para contención de amenazas provenientes del ciberespacio en el comercio marítimo de Colombia, el cual se logra por medio de la recolección de información en motores de búsqueda, repositorios, portales web, entre otras herramientas, para su búsqueda como la ciberdelincuencia en el comercio marítimo, tipos de ciberataques y modelos de ciberseguridad en el comercio marítimo.

La documentación consultada permitió establecer los criterios de selección del modelo, es decir, definir qué características debe tener el modelo teniendo en cuenta las necesidades identificadas en el objetivo anterior, de igual manera, identificar los modelos de ciberseguridad implementados en el mundo para la contención de amenazas provenientes del ciberespacio, ponderar los modelos identificados y de esta manera definir cuál es el modelo más aplicable, o cuál es la propuesta de modelo adaptado a la necesidad.

Es importante mencionar que en esta fase también se lleva a cabo el proceso de análisis documental para estudiar las normas NIST y, así, reconocer los puntos aplicables a la situación del comercio marítimo colombiano en materia de amenazas cibernéticas. De esta forma, se crea un listado de acciones que pudieran aplicarse en la construcción de un modelo enfocado en el caso colombiano y mediante una estructura gráfica que permita explicar y comprender el modelo en profundidad.

Por último, en la tercera fase se verifica el modelo conceptual para el comercio marítimo en Colombia a través de la validación con dos o tres expertos, siendo necesario definir la metodología empleada para dicha validación, así como el perfil del experto con conocimiento, ya sea sobre seguridad cibernética o temas relacionados con el comercio marítimo. De esta manera, y mediante la elaboración de una matriz DOFA, se determinaron las debilidades, oportunidades, fortalezas y amenazas o dar como resultado los aspectos positivos y negativos del modelo propuesto.

Las Amenazas del ciberespacio que afectan la seguridad del comercio marítimo en Colombia

La Teoría del ciberespacio aplicada a la ciberseguridad del comercio marítimo

Estudiar la seguridad ante amenazas provenientes del ciberespacio requiere de una perspectiva teórica que pueda explicar el fenómeno a estudiar, en este caso, la teoría sobre el ciberespacio propuesta por JAdams (2001), la cual es aplicable al tema de estudio

teniendo en cuenta que el autor afirma que "el ciberespacio se ha convertido en un nuevo campo de batalla internacional" (p.6). Se explica desde la perspectiva de la seguridad del comercio marítimo ante amenazas del ciberespacio, como el establecimiento de un nuevo entorno de enfrentamiento en el que las armas y otros escenarios de confrontación pasan a un segundo plano para concentrarse en la evolución de la delincuencia que ahora se establece en un ambiente diferente. Ahora, la confrontación no se da por medio de la guerra física o armamentista, sino que por medio del poder enmarcado en el manejo de la información y datos críticos.

Antecedentes de la Ciberseguridad y el comercio marítimo

En lo que respecta al comercio marítimo, Rodríguez (2016) publica los hallazgos de una investigación sobre la importancia del mar en el mundo contemporáneo y por ende, en el desarrollo del comercio marítimo de los Estados, también, relaciona el uso del océano con la necesidad de fortalecer la seguridad de los mares a través de un concepto de seguridad integral marítima que se interpreta como "un elemento sustantivo, relevante y estratégico para el desarrollo sostenible de los espacios y territorio marítimo nacional." (Rodríguez, 2016, p.41).

Alrededor del tema de la ciberseguridad en el comercio marítimo existen diferentes investigaciones que establecen las bases para otros estudios relacionados, para Moreno (2015), explica la necesidad de manejar un nivel adecuado de ciberseguridad y resiliencia para superar las crisis que se dan a través de las TIC , el objetivo es *potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación* de estos fenómenos que generan inseguridad para la población.

La Compañía Marsh McLennan (2014)contextualiza acerca de los ataques cibernéticos a las organizaciones y las amenazas continuas que se presentan en un entorno en el que las organizaciones necesitan obtener información para conseguir datos que les permitan prevenir cualquier tipo de irrupción. Lo anterior, como consecuencia de un diagnóstico en el que se identifican estructuras preparadas para adaptarse a un espacio cibernético variable y continuo, pero no están listas para enfrentar los ataques y amenazas que se desarrollan con la evolución de las tecnologías y su uso para fines no deseados.

Caracterización de las amenazas provenientes del ciberespacio que afectan la seguridad del comercio marítimo colombiano

Los ataques cibernéticos se pueden presentar por diferentes tipos o técnicas, por ejemplo, pueden ser ataques a contraseñas, ataques por spam, correo, phishing y ataques por malwars, este último el más común cuando se trata de redes que pertenecen a organizaciones, entidades y demás actores involucrados en la actividad comercial marítima y

el que lleva al análisis de riesgos, el cual, está basado en la identificación de amenazas, vulnerabilidades y los riesgos mismos (Valbuena, 2022).

Así mismo, la revisión documental contribuye con la identificación de características relacionadas con las amenazas que, desde el punto de vista de autores como Mednikarov, Tsonev y Lázarov (2020), surgen en los procesos de intercambio de información y en la relación interconectada existentes entre los recursos y sistemas operativos integrados con las plataformas de TI[1]. Para estos autores, las amenazas cibernéticas pueden ser dirigidas y no dirigidas[2], también, se desarrollan en cuatro etapas:

Figura 1. Etapas del ciberataque en la industria marítima

Nota. Estas etapas son aplicables a los buques utilizados para el transporte de mercancías

Fuente: Elaboración propia

Por otro lado, De la Peña (2021), citando a Dingeldey (2017), muestra que los puertos son más vulnerables ante este tipo de ataque cibernético, lo anterior como resultado de la facilidad para ejecutar este tipo de acciones en contra de los sistemas de las navieras a través de Wi-Fi y otras redes, por lo tanto, este estudio se enfoca en las amenazas que se materializan a través de los hechos que afectan a los puertos.

1 Tecnología de la información

2 Los ataques dirigidos son "ataques cibernéticos en redes de Internet corporativas específicas y componentes de red con un propósito específico de penetración: acceso a información confidencial, obstrucción del funcionamiento normal de los sistemas del barco", mientras que los ataques no dirigidos son aquellos que se realizan por medio de "el entorno de Internet y herramientas de software para detectar componentes de comunicación desprotegidos" (Mednikarov, Tsonev, y Lázarov, 2020).

Las amenazas a la seguridad y, por lo tanto, aplicables en este estudio, se clasifican en humanas y lógicas, las primeras hacen referencia a los tipos de ataques provenientes de personas que aprovechan las vulnerabilidades detectadas en los sistemas para obtener información de su interés y beneficiarse de estos datos, es así como surge la figura del *Hacker* quien se enfoca en aprender por eso ingresa al sistema solo para satisfacer su curiosidad pero no para borrar alguna información o hurtarla y luego venderla (Universidad Nacional Autónoma de México, 2009).

Los *cracker* son otro tipo de personas que representan una amenaza para la seguridad cibernética y son quienes acceden a los sistemas para causar algún tipo de daño sin un fin determinado, finalmente están los *Phreakers* que aprovechan la vulnerabilidad de las compañías telefónicas en su beneficio (Universidad Nacional Autónoma de México, 2009).

Las amenazas lógicas, las cuales están representadas en técnicas; es decir, programas como malwares, Bugs, o agujeros que son creados con la intención de dañar los sistemas. Algunos ejemplos son los *adware* o publicidad en ventanas emergentes, los *Backdoors* o puertas traseras que se muestran como atajos para ingresar a los sistemas operativos, también están las *bombas lógicas* que son códigos de los programas que al ser activados producen daños en ellos, continúan con los caballos de troya que hace referencia a programas que se hacen pasar por uno y en realidad es otro y con fines maliciosos, también es conocido como troyano (Universidad Nacional Autónoma de México, 2009).

Otros tipos de amenazas lógicas son los *exploits* que aprovechan las vulnerabilidades de los sistemas, los gusanos que se propagan por las redes para aprovechar las vulnerabilidades y crear acciones maliciosas, también están otros ya conocidos como el *malware*¸ el *phishing*, los *spam*, los programas espía y los virus (Universidad Nacional Autónoma de México, 2009).

Ahora bien, el reconocimiento de las amenazas se realiza teniendo en cuenta los aportes de Rodríguez (2016), quien determina que existen amenazas materializadas en riesgos emergentes que siguen tendencias convertidas en retos enmarcados en fenómenos como el terrorismo que se evidencia en los ataques a buques en alta mar, que se suman a la piratería y otras actividades que hacen parte de la globalización y del incremento de la tecnología.

De la misma forma, la clasificación va de acuerdo con su naturaleza, objetivo y recursos, por lo tanto, estas se registran como ciberespionaje, amenazas híbridas, cibercrimen y hacktivismo; de las cuales son aplicables en el comercio marítimo el ciberespionaje, el cibercrimen, el hacktivismo y las amenazas híbridas que buscan la manipulación de la información (Rodríguez, 2016).

A través del análisis documental se identifican amenazas como la extorsión, la piratería digital, el espionaje, la subversión y el terrorismo (Androjna, Brcko, y Greidanus,

2020), cada una de ellas presentes en diferentes situaciones que afectan en su mayoría a las navieras y por supuesto, a los puertos donde estás operan y en donde son manejados los sistemas que tecnifican los procesos de la actividad marítima. A estas se suman el manejo de información falsa, el narcotráfico y otros delitos trasnacionales (University of Miami, 2017).

Entre tanto, en el caso de Colombia, la información obtenida por medio de las entrevistas hechas a personal que labora en el Comando Conjunto Cibernético de las Fuerzas Militares y en el Comando Cibernético Naval, permite identificar otras amenazas y vectores de ataque. En primer lugar, las amenazas que a través de los tipos de ataques afectan a las plataformas tecnológicas de operación (TO), caracterizadas por ser más difíciles de proteger al tener menos protocolos comerciales y con menos estándares de ciberseguridad, lo que empeora con el uso de cajas negras con mucha información para los operadores y, además, son utilizadas por organizaciones de alto nivel (Aponte, 2022).

También están las plataformas de información (TI), que por medio de diferentes técnicas que afectan a los sistemas soportan las operaciones de los puertos y el comercio marítimo para dar cumplimiento su naturaleza comercial (Correa, 2022). D

De la misma forma, de acuerdo con otros entrevistados, es posible encontrar como amenazas comunes al narcotráfico, la ciberdelincuencia y la piratería como las principales amenazas que afectan al comercio y otras actividades marítimas que están relacionadas con las funciones de la DIMAR y del Ministerio de transporte, las cuales son ejecutadas por medio de lo que los entrevistados llaman *Vectores de ataque* y que incluyen: códigos dañinos, intrusiones, compromiso de la información, contenido abusivo y obtención de información.

Así las cosas, es posible identificar casos relacionados con algunas de las principales ciberamenazas que afectan al comercio marítimo:

Tabla 1. Amenazas al comercio marítimo en el mundo y posibles casos

Amenaza	Tipo	Casos
Hacktivismo	Humana	2013: el White Rose of Drax recibe señales falsas al GPS para desviar su rumbo, pero esto no fue percibido en el radar (Crawford Crawford, 2019).
Narcotráfico	Humana - lógica	2011: En el puerto de Amberes (Bélgica) hackean los sistemas y ocultan droga en los contenedores que estaban registrados como carga legítima (Boyes, 2015).
Piratería digital (amenazas híbridas y terrorismo)	Humana – lógica	2022: Ataque a los sistemas del INVIMA para evitar el funcionamiento y las capacidades de almacenamiento del puerto (Portafolio.com, 2022)

Fuente: Elaboración propia.

Lo anterior, aplicado a la seguridad de la información, lleva a realizar la caracterización de las amenazas, tomando como punto de partida el nivel de importancia que cada una de las amenazas tienen en las entidades y el proceso que debe llevar a cabo el sistema afectado en cada organización que se dedica al comercio marítimo en el país. Es así como se caracterizan en un nivel inferior, bajo, medio, alto y superior, teniendo en cuenta el nivel de criticidad y de importancia para la gestión del comercio marítimo (Ver tabla 2).

Tabla 2. Caracterización de las amenazas teniendo en cuenta el nivel de criticidad del sistema afectado

Nivel de Criticidad	Valor	Descripción
Inferior	0,10	Sistemas con funciones sustituibles o no críticas
Bajo	0,25	Sistemas que hacen referencia a un solo proceso
Medio	0,50	Hace referencia a los sistemas que apoyan a varios de los procesos del comercio marítimo
Alto	0,75	Sistemas que hacen parte del área de tecnología y estaciones con funciones importantes
Superior	1,00	Sistemas en estado crítico y con funciones importantes, sino fundamentales para el comercio marítimo

Nota. Tabla elaborada con base en la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información (Centro Cibernético Policial, Vive Digital, & Presidencia de la República, s.f.).

Fuente: Elaboración propia.

De la misma forma, existen otros parámetros para caracterizar las amenazas, estos establecen el nivel de impacto que estas pueden tener en la gestión del comercio marítimo y en los procesos que se relacionan con este (transporte, logística, etc.), estos son: de Alto Impacto, de Medio Impacto y de Bajo Impacto, los cuales se describen de la siguiente manera:

Figura 2. Caracterización de amenazas según el impacto causado en los sistemas

Nota. Esquema elaborado con información obtenida de la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información (s.f.)

Fuente: Elaboración propia.

A partir de la descripción hecha sobre las formas de caracterización, se establece que en esta investigación se realiza un proceso en el que se combina la caracterización; es decir, inicialmente se identifica el nivel de criticidad y de importancia para la gestión del comercio marítimo y posteriormente, con base en los resultados obtenidos de este proceso, se determina el nivel de impacto que puede tener.

Matriz de Caracterización de Amenazas Cibernéticas

La investigación acerca de amenazas provenientes del ciberespacio es un campo de interés para muchos estudiosos como el Capitán Rodríguez (2016), quien se ocupa de analizar la situación de la seguridad cibernética en el país y las amenazas que hacen parte del contexto de la ciberseguridad en las actividades marítimas en Colombia. No obstante, Crawford Crawford (2019), la evidencia de publicaciones que hablen de las amenazas marítimas es escaso, por lo tanto, identificar las amenazas que afectan a este sector de la economía colombiana se torna en una labor difícil, no obstante, con datos obtenidos a través de la revisión documental es posible reconocer las más sobresalientes.

A continuación, se presenta la matriz de caracterización de las amenazas cibernéticas que afectan al comercio marítimo en el país, las cuales, son clasificadas teniendo en cuenta el nivel de criticidad y nivel del impacto que causan en esta actividad económica.

Tabla 3. Matriz de Caracterización de amenazas cibernéticas

Amenaza/Incidente	Tipo de Amenaza	Agente de la Amenaza	Método	Nivel de Criticidad	Impacto
Ciberespionaje (Acceso no autorizado para ver información de interés del adversario)	Humana	Phreaks, Hacker,	Troyano, Malware, programas espía, virus, adware	Superior	Alto
Amenazas Híbridas (Ciberterrorismo, interrupciones de actividades económicas, interrupción de procesos, virus, narcotráfico)	Lógica	Cracker	Exploits, Malware, adware	Superior	Alto
Cibercrimen (Daño a sistemas, robo de información)	Humana	Cracker, Phreakers	Bombas lógicas, Backdoors, Phishing, spam, bugs, adware	Superior	Alto
Hacktivismo (Buscan generar presión a través del bloqueo de sistemas, virus, robo de cuentas, etc.)	Humana	Hacker, Cracker, Phreakers	Malware, phishing, virus, adware	Alto	Alto

Nota. Matriz realizada con información obtenida de la revisión y análisis documental y a partir de la elaboración propia.

Fuente: Elaboración propia.

De acuerdo con la tabla 3, es evidente que cada una de estas amenazas afectan a este sector porque la mayoría de ellas impiden su correcto funcionamiento, perjudicando indirectamente la economía, desarrollo social y la seguridad del país, de los puertos y de los pueblos costeros que dependen del comercio marítimo, también, son un medio a través del que organizaciones criminales extienden su accionar y fortalecen indirectamente los crímenes trasnacionales, exponiendo vulnerabilidades y nuevas formas de delinquir que esta vez interfieren en la cuarta industria o en la tecnología.

Necesidades de ciberseguridad para el comercio marítimo colombiano

La revisión documental permite encontrar en países como España puntos de referencia que ayudan a entender aspectos de la ciberseguridad de buques y puertos, los cuales, están enfocados en sistemas de comunicación, administración y control que hacen parte de las Tecnologías de la Información, por lo tanto, muestran diferentes niveles de vulnerabilidad ante ataques cibernéticos que son explicados desde una óptica diferente para detectar cuáles son los puntos más vulnerables dentro del desarrollo de la actividad comercial marítima. Por lo general se concentran en los siguientes elementos: "información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos" (Grupo de Seguridad Marítima, 2020, p.50).

De la misma forma, teniendo en cuenta los aportes hechos por el Grupo de Seguridad Marítima de España (2020), se determina que las dimensiones de la seguridad que resultan afectadas a través de los ataques cibernéticos hechos a las actividades del comercio marítimo son:

- La confidencialidad: Indica que la información debe estar disponible solo para quien este autorizado,
- La integridad: Evita que los datos sean modificados,
- La disponibilidad: Permite el acceso a las bases de datos en el momento en el que es necesario,
- La autenticidad: Legitima la veracidad de cada una de las cifras e información que se encuentra en estas bases de datos,
- La responsabilidad de quien manipula estos datos,
- El no repudio: Previene la negación de la autoría de los datos y la fiabilidad que lleva a evitar resultados poco confiables (p.6).

En Colombia, el interés por conocer, identificar y estudiar las amenazas que impactan la Seguridad Integral Marítima y Fluvial se evidencia en la Estrategia de Seguridad Nacional Marítima y Fluvial 2020-2030 creada por el Curso de Altos Estudios Militares (CAEM) No.61 (Curso de Altos Estudios Militares No.61, 2020), investigación que cuenta

dentro de sus hallazgos, amenazas a la seguridad marítima y fluvial relacionadas con el Crimen Trasnacional Organizado y dentro de las que se encuentran algunas relacionadas con las amenazas que afectan la ciberseguridad (p.58).

Las amenazas que son incluidas en este estudio del CAEM son, en primer lugar, los Grupos Armados Organizados que, si bien es cierto, basan su accionar en la violencia, en los últimos años han sido capaces de desarrollar estrategias para practicar el terrorismo por otros medios, incluyendo los cibernéticos, lo que lleva a encontrar en el terrorismo otra de las amenazas que paulatinamente se materializa a través de otros delitos de naturaleza virtual. También existen otras amenazas como la vulnerabilidad de las infraestructuras críticas (security), el hurto en el mar y los ataques a la seguridad cibernética (Curso de Altos Estudios Militares No.61, 2020).

Por otro lado, las respuestas recibidas en medio del desarrollo de las entrevistas aplicadas a personas que tienen experiencia en ese medio, evidencian que los avances de las políticas públicas en materia de ciberseguridad en las actividades comerciales marítimas se encuentra en un proceso lento y que exterioriza varias necesidades. Por ejemplo, la implementación de planes con los que sea posible, desde la labor de la Armada Nacional, llevar una estadística como parte de un sistema de alarmas y establecer cuál de las amenazas que pudieran estás afectado a los buques y demás embarcaciones, de esta forma es posible crear una base de datos que sea de conocimiento de las autoridades portuarias y marítimas y con la que es posible confirmar cuáles son las actividades delictivas más recurrentes en los puertos y mares de Colombia.

También, expresan la necesidad de fortalecer el Comando Cibernético Naval en capacidades de ciberseguridad de unidades marítimas, de esta forma generan estrategias que indirectamente pueden ser útiles en la protección de los buques que transportan mercancía, además, es necesario el fortalecimiento de las capacidades de seguridad cibernética de la Dirección de Tecnologías de la Información que gestiona la Armada Nacional para operaciones navales orientadas al libre desarrollo del comercio marítimo, lo anterior teniendo en cuenta que el Comando cibernético Naval enfoca sus esfuerzos en la protección de la plataforma institucional (Jefatura de Planeación Naval y Dirección de Planeación Estratégica, 2021), pero no tiene programas para el apoyo de la ciberseguridad del comercio marítimo.

De la misma forma, es importante establecer medidas con las que se pueda proteger las bases de datos de las empresas que pueden parecer vulnerables ante ciberdelitos, como el control y el monitoreo de cargas; también es necesario el fortalecimiento y consolidación del principio de corresponsabilidad que atañe a todas las autoridades responsables de la seguridad portuaria y marítima de este tipo de empresas que se encargan del transporte de mercancías por el mar.

Lo anterior, es apoyado por Rivera-Páez y Pérez (2012), quienes afirman que existen necesidades que son notables, por ejemplo:

> […] el continuo intercambio de información entre las instituciones del Estado y sus pares en los estados que son socios comerciales marítimos. La adecuada integración entre las instituciones parte permitirá un intercambio fluido de información que contribuya a mejorar los controles y, por tanto, la seguridad de las actividades marítimas en Colombia. (p.161)

De la misma forma, se establece que en materia de ciberseguridad ante las amenazas que pueden afectar el comercio marítimo en el país, es necesario que en el país acelere la transformación tecnológica en el sector marítimo, lo que quiere decir que la necesidad de reforzar las medidas de seguridad implementadas por las autoridades competentes, incluyendo la Armada Nacional, las cuales son las responsables de prevenir cualquier tipo de ataque tecnológico que pudieran sufrir estas embarcaciones dentro de sus sistemas, o los puertos en materia de GPS.

Modelo conceptual de ciberseguridad para contención de amenazas provenientes del ciberespacio en el comercio marítimo de Colombia

Criterios de selección del modelo aplicable al comercio marítimo

Los elementos a tener en cuenta dentro del estudio para determinar cuál de los modelos aplicables al caso colombiano es el más apropiado, se tienen en cuenta los siguientes aspectos: Tiempo de implementación, resultados parciales o totales, recursos necesarios para su implementación, contexto en donde es aplicado y proceso de implementación, los cuales se describen de la siguiente manera:

- Tiempo de implementación del modelo: Es cierto que un buen trabajo requiere de tiempo, también, de un proceso de pruebas y evaluaciones que permiten perfeccionarlo y adaptarlo a las necesidades de la problemática, que en este caso hace referencia a las amenazas cibernéticas que el comercio marítimo enfrenta en el país. El tiempo de implementación hace referencia al tiempo que tardó este modelo en ser implementado y perfeccionado, ya que es innegable que a mayor tiempo mayor van a ser los costes de este.
- Resultados parciales o totales: Los resultados son uno de los criterios con mayor importancia dentro del análisis, por cuanto a través de ellos es posible verificar la eficacia del modelo y de cada una de las acciones que hacen parte de él, el modelo que presente los mejores resultados a un menor costo puede ser el más conveniente para afrontar la problemática en Colombia.
- Recursos necesarios: Dentro de los dos criterios anteriores, los costes han sido un factor importante a tener en cuenta en el momento de analizarlo, por eso, se

establece este aspecto como parte del análisis del modelo, ya que solo así se puede verificar si los recursos con los que cuenta la Armada Nacional y el país son suficientes, en otras palabras, de esta manera se confirma si este es un modelo económicamente viable para el país.

- Contexto en el que se aplica: Colombia es un país caracterizado por un conflicto armado constante, por lo tanto, cuenta con características y necesidades especiales que no están presentes en todas las Naciones y contextos, por lo tanto, es importante elegir o tener en cuenta un modelo que pueda ser adaptado al entorno colombiano y a las particularidades que genera el conflicto armado, la transición de gobierno y la situación de orden público en el país.
- Proceso de implementación: Este punto se refiere a las fases que deben ser puestas en marcha para aplicar el modelo en su totalidad, en este caso, aquel modelo que muestre un proceso más largo puede ser sinónimo de desventaja para Colombia, ya que puede incurrir en mayores costos económicos y humanos.

La evaluación de cada uno de los modelos se realiza por medio de una ponderación, la cual, se presenta a través de una matriz (Ver tabla 4) que se explica de la siguiente manera: El peso de cada uno de los criterios se mide entre 1-10, donde los números del 1-3 representan que no tienen mayor importancia, los números del 4-7 que tienen una importancia media y del 8- 10 una importancia alta. Así mismo, la puntuación dada a cada uno de los criterios evaluados dentro de cada modelo se basa en la similitud que el contexto tiene con el contexto colombiano, mayor o menor tiempo de aplicación, los costes y necesidades resueltas, por eso, la ponderación tiene una variación entre 1 y 10 donde los números del 1-3 representan una pertinencia poco favorable, los números del 4-7 que medianamente podría satisfacer las necesidades en la ciberseguridad del comercio marítimo en Colombia y del 8- 10 un nivel de pertinencia alto en cada uno de los aspectos analizados.

Modelos de Ciberseguridad aplicables en el comercio marítimo en Colombia

Los modelos de ciberseguridad son el resultado de las necesidades que se generan con la llegada de la pandemia y los ciberataques incrementan haciendo evidentes las vulnerabilidades de los sistemas (Banco Interamericano de Desarrollo - BID & Organización de Estados Americanos -OEA, 2020), es por esta razón que diferentes gobiernos y organizaciones los crean para hacer frente a las amenazas que provienen del ciberespacio y que se encuentran latentes en un mundo cada vez más tecnificado.

Los escenarios planteados en cada uno de los modelos a analizar guardan cierta similitud con la situación Colombiana, además, cumplen en su mayoría con los criterios

de selección establecidos para determinar su pertinencia o la utilidad de sus acciones en el caso colombiano. Es a partir de la verificación de estos puntos que se considera pertinente tener en cuenta los siguientes modelos:

- Modelo de Cooperación en Ciberseguridad
- Modelo de Defensa en Capas
- Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM)

En primer lugar, el Modelo de Cooperación en Ciberseguridad es creado para minimizar los efectos de los ciberataques a través de la implementación de mecanismos que ayuden a prevenir o minimizar el daño que trae consigo una amenaza de ciberataque, eliminando las posibilidades de convertirlas en un riesgo o un ataque real (Guiora, 2018, p.1).

Ante este modelo, Guiora (2018) afirma que su propósito es:

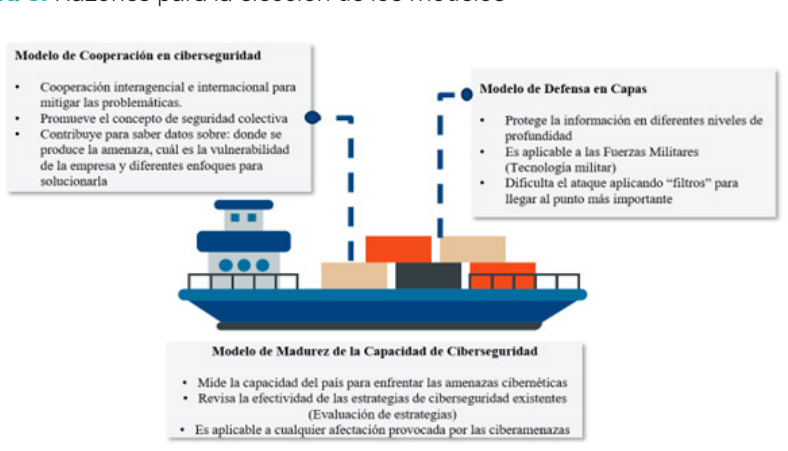
> reducir los costes, tanto directos como indirectos, de las acciones en el ciberespacio. El modelo se fundamenta en una premisa: prevenir un ataque o, en el peor de los casos, llevar a cabo un esfuerzo concertado y decidido es preferible a asumir los costes de un ataque exitoso. (p.03)

Existe otro modelo conocido como el Modelo de Defensa en Capas con el cual se pretende evitar que los ataques provocados en la red puedan expandirse para causar un daño de mayor impacto y además critico dentro de los procesos productivos (Comisión Económica para América Latina y el Caribe, 2020) o, visto desde el caso del comercio marítimo, en los procesos de transporte y distribución de los productos hacía los diferentes puertos del mundo.

Un tercer modelo es el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM), con el cual se espera medir las capacidades de los Estados miembro de la OEA para enfrentar las amenazas provenientes del ciberespacio; este modelo se concentra en cinco dimensiones: "(i) política y estrategia; (ii) cultura y sociedad; (iii) educación, capacitación y habilidades; (iv) marcos legales y regulatorios, y (v) estándares, organizaciones y tecnologías" (Banco Interamericano de Desarrollo - BID y Organización de Estados Americanos -OEA, 2020, p. 15).

Por último, la elección de estos modelos depende, además, de la revisión de los criterios de selección de características que aplican al estudio y al contexto colombiano, los cuales se explican de la siguiente manera:

Figura 3. Razones para la elección de los modelos



Fuente: Elaboración propia.

Ponderación de los modelos

Tomando como referencia los criterios de evaluación planteados de acuerdo con las necesidades de la ciberseguridad del comercio marítimo en los puertos de Colombia, la ponderación de cada uno de los modelos es el siguiente:

Tabla 4. Ponderación de los modelos de ciberseguridad analizados

Factores		Opción					
Criterio	Peso	Modelo de Cooperación en Ciberseguridad		Modelo de Defensa en Capas		Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM)	
			Total		Total		Total
Tiempo de implementación	7	8	56	8	56	8	56
Resultados	8	8	64	7	56	9	72
Recursos necesarios	8	8	64	7	56	7	56
Contexto en el que se aplica	8	7	56	6	48	8	64
Proceso de implementación	7	7	49	6	42	7	49
Total			**289**		**258**		**297**
Promedio			**57,8**		**51,6**		**59,4**

Nota. *El peso de cada uno de los criterios se mide entre 1-10, donde los números del 1-3 representan que no tienen mayor importancia, los números del 4-7 que tienen una importancia media y del 8- 10 una importancia alta.

** La puntuación dada a cada uno de los criterios evaluados dentro de cada modelo tiene una variación entre 1 y 10 donde los números del 1-3 representan que no tiene similitud, los números del 4-7 que tienen una similitud media y del 8- 10 una similitud alta.

***La calificación dada a cada modelo varía entre 1-10, donde los números del 1-3 representan la peor calificación, los números del 4-7 una calificación media y del 8- 10 una calificación importancia alta.

Fuente: Elaboración propia.

De acuerdo con los resultados obtenidos en esta matriz, es posible afirmar que el modelo que cuenta con un mayor número de características que pudieran ser aplicables para la ciberseguridad en el comercio marítimo de Colombia es el de la Madurez de la Capacidad de Ciberseguridad para las Naciones, esto se debe a que analiza cinco dimensiones con las que es posible identificar las debilidades del Estado Colombiano para enfrentar este tipo de amenazas y con base en esta información, crear estrategias a través de las que se consiga prevenir cualquier tipo de ataque y en casos extremos, evitar que estas amenazas se transformen en riesgos.

Modelo aplicable: Modelo de ciberseguridad para el comercio marítimo en los puertos de Colombia

Aspectos Generales

La misión de la Armada Nacional determina que esta institución debe "Desarrollar operaciones navales para la defensa y seguridad nacional, y la protección de los intereses marítimos y fluviales, contribuyendo al desarrollo sostenible del Estado" (Armada Nacional, 2022, párrafo 2). Por lo tanto, hace parte de las funciones de esta institución el desarrollo de estrategias que coadyuven con la protección de los intereses nacionales, los cuales, están dirigidos a la promoción de la cultura marítima colombiana y de su apropiación para crear oportunidades de crecimiento económico sostenible e inclusivo que contribuyan con el desarrollo del país (Ramírez, Pedroza, y Forero, 2021).

El Comercio Marítimo y los Intereses Marítimos en Colombia

El transporte marítimo es una de las actividades que hacen parte de las principales tendencias en la actualidad, su nivel de importancia llega a un punto en el que el 98% del comercio internacional circula por vías marítimas y fluviales del país (Nyman, 2019). Aunque en el año 2018 el comercio marítimo se dio a la baja, de acuerdo con la United Nations Conference on Trade and Development (UNCTAD) genere en la posibilidad de una proyección orientada a un crecimiento del 3,5% entre 2019 y 2024 (United Nations Conference on Trade and Development (UNCTAD), 2019).

Respecto a Colombia, es posible afirmar que

> por sus características geográficas y posición estratégica, se convierte en un país marítimo; en el mar Caribe tiene 658 000 km2 y 330 000 km2 en el Pacífico, lo que representa el 44,8% de la extensión total del territorio, y le da una proyección internacional importante, si se desarrollan las estrategias adecuadas. (Comisión Colombiana del Océano, 2014).

Hasta ahora ha sido posible explicar la importancia que el comercio marítimo tiene para el país desde el punto de vista económico, no obstante, su relevancia también

es visible desde la perspectiva institucional, en la que se determina que como parte de la inteligencia naval, enmarcada en las acciones implementadas por la Jefatura de Inteligencia Naval, se buscan oportunidades que contribuyan con el desarrollo de factores relacionados con la defensa y seguridad de Colombia, por eso, dentro de sus objetivos se encuentra:

> [...] el ingreso al sistema de puertos y la protección del comercio ante la intención de las organizaciones de delincuencia trasnacional de contaminar la carga lícita con estupefacientes. Ese es un fenómeno que de continuar podría tener repercusiones en el comercio exterior y la economía del país. (Jefatura de Planeación Naval y Dirección de Planeación Estratégica, 2021, p. 23)

Así mismo, la Jefatura de Inteligencia Naval considera que:

> La defensa y seguridad tienen nuevos campos de guerra como el ciberespacio, en ese sentido la Armada Nacional, ha conseguido avances en materia de ciberseguridad, ciberdefensa y ciberinteligencia, que han ayudado al aumento en las capacidades de detección, gestión y análisis de eventos e incidentes cibernéticos en la red de datos de la Armada Nacional. (Jefatura de Planeación Naval y Dirección de Planeación Estratégica, 2021, p. 53)

Es evidente entonces que el interés de la Armada Nacional está orientado a la minimización de elementos que desde el ciberespacio afectan la defensa y seguridad de los mares y ríos, así mismo, han entrado en funcionamiento el Centro de Operación de Seguridad (SOC) y un Sistema de Información de Gestión de Eventos (SIEM), desde donde la evaluación y revisión de vulnerabilidades es posible. Es importante generar estrategias con las cuales, esa intención de detener la expansión de la criminalidad a través del espacio marítimo y cibernético se dirija al comercio marítimo, unas de las actividades más importante para la economía colombiana y que pudiera resultar más afectado por estas actividades cibernéticas ilícitas.

Por otro lado, dentro del documento, la Vicepresidencia de la República representada por la Comisión Colombiana del Océano, se establece una lista de 18 intereses, de la misma forma que establecen una clasificación y ejes que se relacionan con estos intereses y, por ende, con la labor de la Armada Nacional (2015).

Teniendo en cuenta lo anterior, este modelo se formula enfocándose en la contribución que la Armada Nacional da a la defensa y seguridad de los mares, haciendo énfasis en dos intereses específicos: La seguridad Integral Marítima y Fluvial (SIMF)[3] y el

3 Es incluida dentro de los intereses marítimos nacionales, este se define como: la gestión conjunta, coordinada e interinstitucional, con la participación de los usuarios, para articular esfuerzos y capacidades, con el propósito de prevenir, proteger y responder ante los riesgos, amenazas y delitos en el dominio marítimo y fluvial que afectan las condiciones de seguridad de las personas, los bienes, los activos y el medio ambiente. (Ramírez, Pedroza, y Forero, 2021, p. 31).

Transporte y comercio marítimo[4], los cuales, se complementan con los siguientes ejes y objetivos CONPES 3990[5] (Ramírez, Pedroza, y Forero, 2021, p.39):

- Ejes estratégicos Política Nacional del Océano y los Espacios Costeros: Integridad y Desarrollo del territorio marítimo y Desarrollo Económico.
- Ejes Estratégicos de la Comisión Colombiana del Océano: Desarrollo fluvial, Seguridad Marítima Integral y Abanderamiento de buques.
- Objetivos CONPES 3990: Incrementar la capacidad del Estado para velar por la soberanía, defensa, vigilancia, control, y seguridad integral marítima e Impulsar las actividades económicas marítimas en función del desarrollo sostenible, local y nacional.

Sin embargo, ninguno de los intereses marítimos está relacionado con la seguridad cibernética, razón por la que esta información tuvo que ser adaptada a las necesidades cibernéticas del comercio marítimo colombiano.

Descripción del Modelo

En el siguiente gráfico se describen los elementos, políticas, entidades, estrategias y planes o campañas que se vinculan a este modelo que tiene como principal objetivo: Definir acciones para la disminución y prevención de amenazas cibernéticas que afecten la operación del comercio marítimo en Colombia.

El modelo está organizado en tres componentes: Metodología de implementación, la Cooperación en ciberseguridad y la Normatividad y Políticas públicas en las que se apoya el desarrollo de las acciones implementadas dentro de este. En primer lugar, la metodología de implementación busca relacionar la misión de la Armada Nacional con la ciberseguridad adaptada a los intereses marítimos de la Nación: Seguridad Integral Marítima y Fluvial (SIMF) y el Transporte y Comercio Marítimo, por lo tanto, los ejes estratégicos a los que se dirige el modelo son: Integridad y proyección del territorio marítimo y el desarrollo económico.

4 El interés enfocado en el transporte y comercio marítimo es explicado como la "Utilización del mar para el transporte seguro de mercancías, sustancias y/o elementos a través de buques versátiles, infraestructura portuaria eficiente, localizada y segura." (p. 32).

5 El Documento CONPES 3990 "Colombia Potencia Bioceánica Sostenible 2030" (2020), posiciona a los océanos dentro de la agenda pública nacional como factores que contribuyen con el desarrollo sostenible del país en los próximos 11 años, lo anterior basados en la siguiente consigna: los estados ejercen soberanía; aprovechan su posición geopolítica, sus ecosistemas marinos y su biodiversidad; hacen uso de los accesos a los océanos y las líneas marítimas; realizan actividades marítimas sostenibles y competitivas; generan capacidad naval, conocimiento y conciencia nacional oceánica; defienden los intereses marítimos nacionales, y gestionan interinstitucionalmente de los océanos (Mahan, 1980; Till, Seapower: A Guide for the Twenty-First Century, 2004). (Consejo Nacional de Política Económica y Social CONPES, 2020)

Figura 4. Esquema gráfico del Modelo de ciberseguridad para el comercio marítimo en los puertos de Colombia

Fuente: Elaboración propia

Componente: Metodología de implementación

Dentro del componente de la metodología de implementación también se habla de los gerentes del modelo, en otras palabras, los responsables, quienes teniendo en cuenta lo establecido en el documento *Intereses Marítimos* de Colombia (2021) son: Ministerio de Defensa Nacional, la Dirección General Marítima (2021) y la Armada de Colombia. El componente que habla de la implementación del modelo se basa en el Marco de Seguridad Cibernética de NIST[6] Cibersecurity Framework, razón por la que se desarrolla por medio de cinco áreas estratégicas, cada una de ellas con acciones específicas que se crean a

6 El NIST es una "infraestructura de seguridad cibernética" que tiene como finalidad ayudar a las organizaciones a mejorar o implementar acciones para la ciberseguridad a través de la gestión de riesgos y la resistencia de sus sistemas (Amazon Web Services, Inc, 2019).

partir de las necesidades en materia de ciberseguridad para el comercio marítimo en Colombia (Ver tabla 5).

Tabla 5. Áreas funcionales y acciones para implementar en el modelo

Función	Acción
Identificar	Identificación y clasificación de sistemas e información sensible de las navieras y puertos. Identificación de vulnerabilidades y amenazas en los sistemas de los puertos. Identificación de procesos, permisos de acceso y personas responsables a las bases de datos y sistemas de los puertos.
Proteger	Proteger el acceso a información sensible de navieras y puertos. Proteger Servicios operacionales importantes dentro de los procesos logísticos del comercio marítimo Proteger sistemas de información y operacionales relacionados con las plataformas operativas y de la información de los puertos. Proteger cuentas y bases de datos que pueden ser vulnerables
Detectar	Detectar los intentos de ataques cibernéticos llevados a cabo en los últimos seis meses a través de la conexión existente con el Centro de Operación de Seguridad (SOC) y un Sistema de Información de Gestión de Eventos (SIEM). Detectar los Ataques cibernéticos efectuados en el último semestre por medio del trabajo interagencial y la conexión con el Centro de Operación de Seguridad (SOC) y un Sistema de Información de Gestión de Eventos (SIEM). Detectar cuantas, y cuales amenazas emitidas son dirigidas a entidades estatales, empresas que trabajan en el puerto e incluso, a la Armada de Colombia a través de elementos relacionados con el comercio marítimo y que pudieron ser detectadas en el Centro de Operación de Seguridad (SOC) y un Sistema de Información de Gestión de Eventos (SIEM).
Responder	Elaborando informes y mostrando pruebas con las que se certifique la existencia de los incidentes de ciberseguridad detectados.
Recuperar	Recuperar cuentas y acceso a sistemas bloqueados en el menor tiempo posible y generando un bloqueo para que solo puedan acceder con un código específico. Recuperar el acceso a las bases de datos que han sido irrumpidas en el menor tiempo posible, evitando que los datos puedan ser vistos o extraídos por algún método. Recuperar el control para garantizar la continuidad de los procesos del comercio marítimo.

Fuente: Elaboración propia

Componente: Cooperación en ciberseguridad

La cooperación en ciberseguridad es un proceso que depende del trabajo interinstitucional, es decir, de las estrategias o planes implementados por la DIMAR y la Armada Nacional y que necesitan del apoyo de otras instituciones como la Comisión Colombiana del Océano, la Vicepresidencia de la República, organizaciones dedicadas al comercio marítimo y al trabajo en los puertos, el Ministerio de Defensa a través de la Fuerza Pública (Policía Nacional, Fuerza Aérea) y la Dirección Marítima por medio de otras unidades que no se ocupen de la ciberdefensa y la ciberseguridad, las cuales cuentan con información, herramientas o incluso, tecnología, que pueda ser de ayuda para la prevención e irrupción de delitos cometidos en contra del comercio marítimo a través del ciberespacio.

Es importante mencionar que dentro de la Cooperación en Ciberseguridad existe la necesidad de establecer contacto con las entidades y gobiernos de otros países para que se logre hacer un trabajo coordinado cuando se trata de organizaciones que irrumpen en los sistemas nacionales y operan desde otras partes del mundo, o, cuando el caso es al contrario, el trabajo coordinado con otros países permite a la Armada Nacional al defensa de los intereses marítimo de Colombia y con ello, salvaguardar la soberanía del país.

Componente: Normatividad y Políticas Públicas

En este componente se incluyen las políticas y normas que rigen el modelo y sirven como punto de partida para la formulación del modelo y la definición de las acciones que hacen parte de cada una de las áreas funcionales de este, las políticas y normas vinculadas al modelo se clasifican según su ámbito de aplicación en nacionales, cibernéticas y marítimas o fluviales. A este componente pertenecen:

- Nacionales: El Plan Nacional de Desarrollo, la Política de Defensa y Seguridad, la Política Nacional Logística y el documento que consigna los intereses marítimos de Colombia.
- Marítimos y fluviales: Política Nacional del Océano y los Espacios Costeros
- Cibernéticos: Marco NIST y el Decreto 338 de 2022

Evaluación de la aplicación del modelo

Una vez implementado el modelo se realizará un seguimiento trimestral y semestral para revisar qué parte del modelo muestra mayor efectividad y si existe una minimización de los incidentes y ataques que hasta el momento habían sido detectados gracias a las alertas tempranas o a las denuncias hechas por las navieras y trabajadores de los puertos. Es así como se establece que los indicadores para determinar cuáles son los cambios que se generan alrededor de este y los que permiten disminuir el impacto que la delincuencia causa en la seguridad cibernética de los puertos de Colombia, estos son:

$$\frac{\textit{(\# de ataques identificados en el SOC y SIEM)}}{\textit{(\# de ataques prevenidos)}}$$

De esta manera será posible comprobar de forma continua, la efectividad de las acciones implementadas como parte del modelo, claro está, la evaluación del modelo en esta oportunidad se hace desde la perspectiva de la prevención de problemáticas que pudieran relacionarse con amenazas como narcotráfico, ciberdelincuencia, hacktivismo, entre otros.

$$\frac{\textit{(\# de denuncias recibidas por ataques identificados)}}{\textit{(\# de ataques presentados durante tres meses)}}$$

Verificar semestralmente el número de ataques perpetrados y con resultados negativos para el comercio marítimo establece un punto de partida para determinar la existencia del trabajo coordinado con los empresarios y las directivas de los puertos, así mismo, teniendo en cuenta que dentro del modelo existe un componente enfocado en la cooperación en ciberseguridad, por medio de la conexión con el Centro Cibernético Policial y la Unidad de Delitos Cibernéticos, para saber cuántas denuncias por estos hechos se está realizando un trabajo interinstitucional con la Policía Nacional.

De esta manera, es posible confirmar que la cooperación en ciberseguridad es una herramienta efectiva cuando se trata de reducir la presencia de organizaciones criminales que operan en los sistemas de los puertos, también, revisar cuantas personas cumplen con la denuncia y contribuyen con ella para que las autoridades procedan de inmediato.

Dentro de la evaluación de la efectividad del modelo también se tendrán en cuenta, de forma trimestral, la discriminación de las novedades dependiendo el tipo de ataque que es llevado a cabo, el sistema que ha sido atacado y la cantidad de veces que han intentado vulnerarlo, de esta forma es posible identificar los puntos débiles dentro del sistema del puerto y también. La manera como la ciberdelincuencia está siendo ejecutada, también si existe la posibilidad que esta utilice más de un tipo de ataque al mismo tiempo y de qué forma la DIMAR e incluso, la misma Armada Nacional a través de los centros estratégicos que ahora trabajarían de forma coordinada con los de la DIMAR, han logrado impedir al menos con la alerta, posibles ataques cibernéticos.

Estos indicadores funcionan como un plan piloto y guía para desarrollar otros que permitan ver la efectividad del modelo y también, realizar un proceso de retroalimentación semestral para que contribuya con la disminución de irrupciones hechas en los sistemas del comercio marítimo en los puertos de Colombia.

Validación del modelo

La validación del modelo se realiza desde dos puntos de vista, el primero de ellos es el que aporta una matriz DOFA, con la cual se revisan las debilidades, oportunidades, fortalezas y amenazas para esta propuesta. La segunda perspectiva la proveen las opiniones de expertos que son docentes y conocedores de la materia que han trabajado con temas relacionados al objeto de este estudio.

Matriz DOFA

Tabla 6. Matriz DOFA Modelo

MATRIZ DOFA	FORTALEZAS (F)	DEBILIDADES (D)
	1. Análisis de amenazas nacionales teniendo en cuenta sucesos recientes (INVIMA), también la perspectiva de personal que labora en unidades relacionadas con la ciberseguridad. 2. Experiencia y conocimiento del personal entrevistado y que aporta información para crear el modelo. 3. La creación del Centro de Operación de Seguridad (SOC) y del Sistema de Información y Gestión (SIEM), con los que la Armada Nacional puede contribuir en materia de ciberseguridad en el mar.	1. Escasez de documentación o investigaciones previas que proporcionen información relacionada con el tema de las ciberamenazas al comercio marítimo y de la Ciberseguridad en el mar 2. El enfoque del modelo inicialmente se concentra solo en los puertos y en las novedades relacionadas con la ciberseguridad en sus sistemas 3. En la implementación del modelo, la falta de capacitación del personal para el manejo de sistemas y equipos que puedan establecer alguna conexión con otras entidades, instituciones y navieras
OPORTUNIDADES (O)	**ESTRATÉGIA (FO)**	**ESTRATÉGIAS (DO)**
1. Normatividad y programas gubernamentales relacionados con la gobernabilidad cibernética. 2. El Plan de Desarrollo Naval que con miras al año 2042 plantea estrategias que se orientan a la seguridad cibernética y cómo debe ser implementada en favor de los intereses de los colombianos 3. Vinculación de las autoridades y entidades competentes dentro del modelo para realizar un trabajo coordinado que complemente actividades y fortalezca los procesos de protección de la ciberseguridad.	1. Aprovechar la experiencia y el conocimiento del personal entrevistado para identificar las necesidades en materia de ciberseguridad del comercio marítimo, a partir del trabajo coordinado, las iniciativas gubernamentales y los planes de la Armada Nacional para ampliar el alcance de la labor de la institución llegando a la ciberseguridad de las navieras y otras instituciones que podrían resultar afectadas por amenazas cibernéticas desde la labor hecha en el SOC y en el SIEM	1. Incentivar la investigación desde la Armada Nacional dirigida a la ciberseguridad en espacios marítimos, lo anterior teniendo en cuenta que es importante tener datos e información que pueda aportar pistas sobre las amenazas que no solo afectan al comercio marítimo, también pueden ser amenazas para la Institución y otras entidades gubernamentales que son vulnerables ante este tipo de ataques.
AMENAZAS (A)	**ESTRATEGIAS (FA)**	**ESTRATEGIAS (DA)**
1. Con la llegada de un nuevo gobierno puede haber cambios en las políticas públicas relacionadas con la ciberseguridad, la protección de los intereses marítimos y otros aspectos relacionados con la ciberseguridad y el comercio marítimo.	1. La experiencia y el conocimiento del personal entrevistado y que labora en las unidades relacionadas con la ciberseguridad de la Armada Nacional puede llevar a establecer estrategias y acciones con las que se fomente la ciberseguridad y la	1. Buscar la oportunidad en medio de las políticas gubernamentales y la normatividad nacional para generar investigaciones que fortalezcan la ciberseguridad en el espacio marítimo colombiano, también, para capacitar al personal en la manera

Continúa tabla...

AMENAZAS (A)	ESTRATEGIAS (FA)	ESTRATEGIAS (DA)
2. Negación a la cooperación interagencial e internacional para proporcionar información o trabajar de forma coordinada. 3. Proyección y mutación del ciberdelito basados en los avances tecnológicos, el acceso a programas e información para bloquear la actividad marítima comercial	cooperación en ciberseguridad, está última vista como una opción para prevenir la mutación del ciberdelito y del cibercrimen que afectan en la actualidad a las navieras y con ello, a la ciberseguridad, un nuevo espacio que debe ser protegido para ver por la seguridad nacional.	como deben manejar la información que se encuentra en el ciberespacio, como blindarla y eliminar las vulnerabilidades que pudieran ser la puerta de entrada para hackers, evitando así la proyección de sus delitos y del desarrollo de las ciberamenazas.

Fuente: Elaboración propia

El segundo punto de vista en la validación del documento es aportado por personal experto o conocedor del tema teniendo en cuenta que laboran en unidades relacionadas con la ciberseguridad de alguna de las Fuerzas Armadas de Colombia o cuentan con estudios relacionados en el tema, estas personas evalúan la viabilidad y pertinencia del modelo teniendo en cuenta el objetivo de la investigación y la problemática planteada en este. La evaluación se realiza sobre ítems como los componentes del modelo, la aplicación del Marco Normativo NIST y su pertinencia, teniendo en cuenta la situación actual de la seguridad cibernética en el comercio marítimo del país.

Conclusiones

El proceso de caracterización de las amenazas que en la actualidad afectan la ciberseguridad en el espacio marítimo fue llevado a cabo teniendo en cuenta la opinión de los entrevistados y expertos en el tema. Lo anterior, como consecuencia de la carencia de documentación que muestre datos recientes relacionados con este tipo de problemáticas; sin embargo, también se tomaron como punto de referencia casos en otros países del mundo.

Es importante mencionar que dentro de la caracterización de las amenazas fue posible encontrar que las amenazas cibernéticas dirigidas a navieras e incluso a entidades gubernamentales se intensificaron luego del año 2020, ya que con la llegada de la pandemia la mayoría de procesos fueron vinculados a algún sistema o proceso cibernético, también, que va más allá del robo de información porque existen delitos trasnacionales como la extorsión o el narcotráfico, los cuales se han beneficiado de estas amenazas para manipular la información del sistema y la información relacionada con la carga de los contenedores o simplemente, saber sus rutas para retener la carga y extorsionar a las navieras.

Por otro lado, la definición del modelo de ciberseguridad es un proceso en el que se toma como punto de referencia modelos de seguridad marítima de países como España,

encontrando diferencias en el manejo que cada país tiene frente a este tipo de situaciones, también mostrando el alcance que la ciberdelincuencia y el cibercrimen, han logrado que la Armada Nacional haga parte de este grupo de autoridades para proteger el espacio cibernético que atañe al mar, pensando en crear un modelo que también se fundamente en el Marco Normativo NIST que tiene sus inicios en Estados Unidos y que puede ser aplicable a empresas como las navieras de Colombia.

Lo que lleva a construir un modelo basado en las lecciones aprendidas de otros países y en la información proporcionada por los expertos sobre las ciberamenazas al comercio marítimo en Colombia, por eso busca prevenirlas y trabajar de forma coordinada para detener las existentes.

La validación del modelo elaborado se realiza desde dos puntos de vista, el primero de ellos es a través de una matriz DOFA con la que se evalúa teniendo en cuenta el entorno, la situación actual de estas amenazas en el país y los hallazgos de esta investigación, el segundo es el punto de vista de expertos que consideran viable el modelo teniendo en cuenta la posibilidad de que la Armada Nacional intervenga en esta problemática siempre y cuando cuente con el apoyo de entidades y organizaciones vinculadas con este sector y así trabajar de forma eficiente.

Finalmente, se realiza una propuesta de un modelo de ciberseguridad aplicable en el comercio marítimo en Colombia y las amenazas provenientes del ciberespacio, el cual, cuenta con tres componentes que promueven acciones para prevenir y detener este tipo de novedades, también vincula la normatividad y políticas existentes en los que se fundamenta para siempre actuar acorde a lo establecido con la Ley y promueve el trabajo coordinado con otras entidades. De esta forma, logra cubrir la mayoría de áreas relacionadas y actuar desde todos los frentes posibles para reducir la actuación de estos grupos delincuenciales que actúan a través del ciberespacio.

Recomendaciones

Con el desarrollo de la investigación fue posible percatarse de la inexistencia de estudios en la Armada Nacional que vayan más allá de los intereses institucionales, por eso, se sugiere la promoción de la investigación enfocada en fenómenos que afectan la seguridad y ciberseguridad marítima desde otras perspectivas como la de las navieras y, de esta forma, identificar que problemas pueden representar una amenazas para la Armada Nacional y la seguridad nacional. Se debe crear una base de datos que pueda ser consultada a la hora de revisar antecedentes que sirvan como punto de partida para la creación de estrategias de seguridad y para próximos estudios.

Declaración de divulgación

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

Autor

Juan Pablo Gómez López. Magister en Ciberseguridad y Ciberdefensa, Colombia. Especialista en Política y Estrategia Marítima y Profesional en Ciencias Navales y Administración de la Escuela Naval "Almirante Padilla", Colombia.

ORCID: https://orcid.org/0000-0001-6657-5251
Contacto: gomezlj@esdeg.edu.co

Referencias

Adams, J. (2001). Virtual Defense. Foreing Affairs, 80(3), 98-112. doi:https://doi.org/10.2307/20050154

Aguirre, J. (2010). Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI. Espéculo. *Revista de Estudios literarios*, 33. https://biblioteca.org.ar/libros/150717.pdf

Amazon Web Services, Inc. (2019). *Marco de Seguridad Cibernética NIST (CSF, por sus siglas en inglés). Alineación con el NIST CSF en la nube de AWS.* Amazon Web.

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering*, 8(10), 776. https://doi.org/10.3390/jmse8100776

Aponte, J. D. (31 de Julio de 2022). *Jefe del Departamento de Prospectiva Cibernética*. (J. Gómez, Entrevistador)

Armada Nacional. (2015). *Plan Estratégico Naval 2015-2018*. Armada Nacional de Colombia.

Armada Nacional. (2022). Misión y Visión. https://www.armada.mil.co

Banco Interamericano de Desarrollo - BID, & Organización de Estados Americanos -OEA. (2020). *Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe. Banco Interamericano de Desarrollo*. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Boyes, H. (2015). Cyber security and cyber-resilient supply chains. *Technology Innovation*, 5(4), 28-34.

Comisión Económica para América Latina y el Caribe. (2020). *La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad. CEPAL*. https://repositorio.cepal.org/bitstream/handle/11362/46275/1/S2000679_es.pdf

Comisión Colombiana del Océano. (2014). *Construyendo País Marítimo*. http://www.cco.gov.co/docs/publicaciones/libro_construyendo_pais_maritimo.pdf.

Consejo Nacional de Política Económica y Social CONPES. (2020). *Documento CONPES 3990 «Colombia Potencia Bioceánica Sostenible 2030»*. Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3990.pdf

Correa, J. (2022). *Entrevista investigación*. (J. Gómez, Entrevistador)

Crawford Crawford, J. (2019). Ciberataque al Transporte Marítimo: ¿Una Amenaza Real o Ciencia Ficción? *Revista de Marina* (970), 15-23. https://revistamarina.cl/revistas/2019/3/jcrawfordc.pdf

Curso de Altos Estudios Militares No.61. (2020). *Estrategia de Seguridad Nacional Marítima y Fluvial*. Primera Edición, 115. Bogotá, Colombia: ESDEGUE - Graphic Motion.

De la Peña, I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue ¨[Online]. *Transport Policy,* 1-4.

Dingeldey, P. (2017). Port Automation and Cybersecurity Risks [On line]. *The Maritime Executive*. https://www.maritime-executive.com/editorials/port-automation-and-cybersecurity-risks

Dirección General Marítima. (2021). Estadísticas Anuales de Transporte Marítimo en Colombia 2020 [Formato Digital] (Primera edición ed.). Bogotá, Colombia: Dimar.

Grimalt, C., & Baró, B. (2021). *Seguridad marítima y portuaria en la era 4.0*. https://www.mapfreglobalrisks.com/gerencia-riesgos-seguros/articulos/seguridad-maritima-y-portuaria-en-la-era-4-0/

Grupo de Seguridad Marítima. (2020). *Guía de Buenas Prácticas para la Gestión de Riesgos de Ciberseguridad en Buques e Instalaciones Portuarias*. Consejo Nacional de Seguridad Marítima.

Guiora, A. (2018). Ciberseguridad: un modelo de cooperación. *OpenMind*, 29. https://www.bbvaopenmind.com/wp-content/uploads/2018/12/BBVA-OpenMind-Amos-Guiora-Ciberseguridad-un-modelo-de-cooperacion.pdf

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). *Metodología de la Investigación* (Sexta Edición ed.). McGrawHill Education.

Jefatura de Planeación Naval, & Dirección de Planeación Estratégica. (2021). *Plan de Desarrollo Naval 2042*. https://www.armada.mil.co/sites/default/files/descargas/Plan%20Desarrollo%20Naval%202042%2007042021.pdf

Marsh McLenann Company. (Julio de 2014). *El riesgo del ciberataque al sector marítimo*. https://www.marsh.com/co/services/cyber-risk/insights/-estan-sus-barcos-protegidos-contra-ataques-ciberneticos-.html

Mednikarov, B., Tsonev, Y., & Lázarov, A. (2020). Analysis of Cybersecurity Issues in the Maritime Industry. *Information & Security*, 41(1), 27-43. doi: https://doi.org/10.11610/isij.4702

Centro Cibernético Policial, Vive Digital, & Presidencia de la República. (s.f.). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información*. MINTIC. https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Moreno, A. (2015). La Estrategia de Seguridad Nacional. Ciberdefensa y Seguridades Marítimas y Energéticas. *Revista General de Marina*, 269, 747-755.

Nyman, E. (2019). Techno-optimism and ocean governance: New trends in maritime monitoring. *Marine Policy*, 30-33. doi:https://doi.org/10.1016/j.marpol.2018.10.027

Portafolio. (2022). Por qué el ataque cibernético al Invima encarecería más los productos. *Portafolio*. https://www.portafolio.co/economia/finanzas/invima-ataque-cibernetico-encareceria-los-productos-en-colombia-561912

Ramírez, F., Pedroza, W., & Forero, J. (2021). *IMC - Intereses Marítimos de Colombia*. Vicepresidencia de la República-Comisión Colombiana del Océano-Armada de Colombia.

Rivera, S., & Pérez, J. (2012). El Transporte Marítimo y las Fronteras Portuarias: Contenedores y Narcotráfico. En *Crimen Organizado Transnacional y Conflictos Ambientales en América* (págs. 121-163). Sello Editorial ESDEG.

Rodríguez, H. (2016). Seguridad Integral Marítima, Reto Estratégico. En H. Rodríguez, L. Osorio, S. Uribe, & L. Chávez, *Seguridad Marítima: Retos y Amenazas* (Primera Edición ed., págs. 9-44). Sello Editorial ESDEG. doi: https://doi.org/10.25062/9789585605480

Universidad Nacional Autónoma de México. (2009). Capítulo 2. Amenazas y vulnerabilidades de la seguridad informática. http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/217/A5.pdf?sequence=5

United Nations Conference on Trade and Development (UNCTAD). (2019). *Review of maritime transport.* https://unctad.org/system/files/official-document/rmt2019_en.pdf

University of Miami. (2017). *Global Threats: Cybersecurity in Ports (Donald Duck, Daughters & Dollars*). Center for International Business Education & Research (CIBER).

Valbuena, M. (2022). *MUSD Caracterización de las Ciberamenazas*. Universidad de Nebrija.

Valvuena, M. (2022). M*undo Cibernético. Unidad Didáctica 2: Caracterización de las ciberamenazas.* Universidad de Nebrija.

Esta página queda intencionalmente en blanco

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 1, número 2, julio-diciembre 2022 (pp. 145-166)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

El ciberespacio como variable habilitante para la movilización de masas y desestabilización del orden público en Colombia

Cyberspace as an enabling variable for mass mobilization and destabilization of public order in Colombia

DOI: https://doi.org/10.25062/2955-0270.4770

Diego Fernando Benjumea Gutiérrez
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

La movilización de masas en Colombia ha sido una práctica constante en el último tiempo, el cual actualmente es ejercido a través del ciberespacio entendido como un lugar sin límites terrestres, sin horarios, sin restricciones, multilingual, anónimo, democrático, libre y con comunicación simultánea, masiva y rápida.

La movilización de masas virtuales se agrupa y se ejerce en las redes sociales en donde se establecen relaciones sociales, se comparten valores, ideales, sentimientos y se convierte en la pizarra digital para manifestar las disconformidades sociales, políticas, económicas y tratar de hacer cumplir derechos y acuerdos con los gobiernos.

En el presente trabajo se estudia el ciberespacio como el medio utilizado por las citadas masas para perturbar el orden público en Colombia.

Palabras Clave: Ciberespacio, Movilización, Movilización social, Redes sociales

Abstract

Mass mobilization in Colombia has been a constant practice in recent times, which is now exercised through cyberspace, understood as a place without terrestrial limits, without schedules, without restrictions, multilingual, anonymous, democratic, free and with simultaneous communication, massive and fast.

The mobilization of virtual masses is grouped and carried out on social networks where social relationships are established, values, ideals, feelings are shared and become the digital blackboard to express social, political and economic disagreements and try to enforce rights. and agreements with governments.

In this work, cyberspace is studied as the means used by the aforementioned masses to disrupt public order in Colombia.

Key words: Cyberspace, Mobilization, Social mobilization, Social networks

Artículo de Debates
Recibido: 25 de agosto de 2022 • **Aceptado:** 16 de noviembre de 2022
Contacto: Diego Fernando Benjumea Gutiérrez benjumead@esdeg.edu.co

Introducción

En el ciberespacio las interacciones se dan en un escenario impersonal, anacrónico, masivo, rápido y simultáneo en donde se comparten intereses, valores e incluso se ejercen derechos. Este se ha convertido en el escenario preferido para entablar cualquier clase de interacción, por cuanto refiere a un aglomerado de dispositivos conectados por redes donde el cibernauta comparte información digital, lo que implica la construcción de relaciones con otra persona o grupo de personas, ya sea social, económica, laboral, educativa y en gran medida personal.

Este artículo centra su atención en argumentar la manera en la que el ciberespacio es una variable habilitante para movilizar las masas y desestabilizar el orden público en Colombia, pretendiendo entender como en la actualidad se construyen las relaciones en este escenario virtual y como los avances tecnológicos van configurando el carácter de estas interacciones, ya sea optimizando o dificultando algunos procesos y resaltando el impacto generacional.

Posterior a ello, se trata de establecer los métodos de acercamiento y movilización de masas a través del ciberespacio, en el cual se analiza la convocatoria que hace un sujeto o un grupo de sujetos por medio de sus redes sociales como son Facebook, Twitter e Instagram, o por videos en YouTube, blogs e incluso plataformas de mensajería instantánea tales como, WhatsApp, Telegram, Signal, Messenger, entre otras.

Finalmente, expuestos los métodos de acercamiento y movilización de masas a través del ciberespacio, se abordan las consecuencias de dicha movilización en el orden público en Colombia, examinando todas las aristas, como el ciberterrorismo, las estructuras del poder, de expresión y la eliminación de decisiones gubernamentales, entre otras.

Metodología

Conforme a lo anterior, se empleó la hermenéutica textual, que de acuerdo a González (2013) es "la teoría de las operaciones de comprensión en su relación con la interpretación de textos, en la que la palabra hermenéutica no significa otra cosa que la experiencia metódica de la interpretación" (p. 59). Para Cárcamo (2005) "un elemento esencial para la comprensión en el proceso de interpretación está dado por la focalización precisa respecto a aquello que se desea interpretar" (p.208).

Por esta razón, se le atribuirá un vínculo de diseño cualitativo interpretativo, desde el enfoque de la etnometodología, la cual, según Ghiso (1996) intenta estudiar los fenómenos sociales incorporados a nuestros discursos y nuestras acciones a través del análisis de las actividades humanas.

Marco teórico y conceptual

Para iniciar con el marco teórico es de interés establecer que la movilización social en palabras de Pérez (2015) se concibe como:

> Un proceso participativo de acciones colectivas orientado a promover, contribuir e impulsar, propuestas alternativas y críticas al modelo de sociedad dominante que ahonden en una mayor justicia social. Este proceso entiende que la transformación pasa por la ocupación y la presencia en los espacios públicos para denunciar, reivindicar, educar y sensibilizar sobre dichas alternativas (Pérez, 2015, párrafo 1).

Asimismo, la movilización social hace parte de un proceso participativo político que se concreta en la protesta social, la cual en palabras de Riaño (2015) se define como "La protesta social es un mecanismo de participación política fundamental para la defensa de los derechos naturales que, pese a su regularización, no deja de ser habitual en el orden mundial contemporáneo" (Riaño, 2018, p 2).

La movilización social como ejercicio de ese mecanismo de participación se puede ejercerse a través del ciberespacio en razón a que este al componerse de infraestructura de tecnologías de la información y datos contenidos que incluyen: internet, telecomunicaciones, redes, sistemas informáticos, procesadores y controladores integrados lo que permite hacer en forma eficiente la convocatoria como el ejercicio del mecanismo participativo citado.

Determinado el medio a través del cual se realiza la movilización social, el término ciberespacio, según Carlini (2018), quien cita a Gibson (1984) se originó en el libro de ciencia ficción Neuromante:

> En su obra, el autor describe una red de computadoras ficticias que contenía una gran cantidad de información que podía explotarse con el fin de adquirir poder y riqueza. En esta novela, los dos mundos se entrelazan hasta que los usuarios humanos perciben experiencias que en realidad no existen y son creadas por los ordenadores. (Gibson, 1984; Carlini, 2018, p. 233).

Además, desde el punto de vista del área donde se ubica el ciberespacio se concibe como la " [...]'desespacialización' [a la que] se le denomina 'ciberespacio', al 'espacio deslocalizado', espacio que debe reconocer el papel fundamental de los medios en el campo de la interacción social". (Pinzón, 2014, p. 28).

Escenario digital es de gran relevancia en la medida en que en ella confluyen las relaciones sociales, por lo cual en palabras de Orihuela (2008) son las redes sociales que comprenden los espacios virtuales en los que nos relacionamos y en los que construimos nuestra identidad, pero también funcionan a modo de sistema de filtro y de alerta en la medida en que permiten un ajuste del flujo de información que recibimos en función de nuestros intereses y de los intereses de aquellos en quienes confiamos (Orihueja, 2008, p. 59-60).

De este modo, la red social como mecanismo de interacción social para Castañeda (2010) se denomina la Red Social Virtual, ya que es "la unión de un grupo de personas que se conectan a través de internet con una finalidad común" (Castañeda, 2010, p. 29).

El empleo del ciberespacio como mecanismo de construcción de relaciones sociales.

Con el desarrollo de las tecnologías digitales en la cotidianidad humana, las relaciones sociales basadas en el uso del ciberespacio, ha demostrado también ser un nuevo espacio para la producción cultural en que las ideas de corporeidad, espacio y tiempo no existen tal como se conciben clásicamente (Mosquera, 2008).

Hoy, todas las actividades de la vida cotidiana se encuentran permeadas por el empleo de las herramientas tecnológicas y, en ellas, el uso del ciberespacio. Desde lo más simple como preparar una comida a lo más complejo como efectuar relaciones comerciales o tomar una clase, se encuentra inmerso en el espacio virtual. Las relaciones sociales como ejercicio de nuestra dimensión social no son ajenas a ellas. El concepto de relación social implica un conjunto de interacciones que ocurren entre dos o más personas, grupo de personas que siguen en forma mutua unos ritos o formalidades aceptados por sus partícipes.

La Real Academia de la Lengua Española (RAE) define la palabra relación en una de sus acepciones como; conexión, correspondencia, trato, comunicación de alguien con otra persona. U. m. en pl. Relaciones de parentesco, de amistad, amorosas, comerciales (La Real Academia de la Lengua Española, s. f.).

De la definición precedente se establece que la relación implica el trato con otra persona sin determinar el medio por el cual se establece. De este modo, en palabras de Grossetti "la relación social entre dos personas puede entonces ser definida como un conocimiento y un compromiso recíprocos fundados sobre interacciones" (Grossetti, 2009, p. 59). Implica que necesariamente que las personas se agrupen en familia, comunidades, estados, organizaciones de acuerdo con nuestras afinidades personales, sociales, religiosas, laborales o políticas.

El espacio virtual o ciberespacio se convierte en el lugar preponderante para iniciar, mantener o concluir las diferentes relaciones sociales. Si bien, los ciudadanos día a día emplean la infraestructura del ciberespacio para el desarrollo de sus actividades cotidianas y ejercer sus relaciones sociales, desconocen su definición, por lo que, resulta precedente establecer su significado.

En este punto, resulta importante indicar que el uso de la red se ha modificado a lo largo de los años; en palabras de Carlini (2018) primero el actor era pasivo, la Web 1.0,

se caracterizaba principalmente por ser unidireccional, realizándose sobre contenidos estáticos, en el cual las páginas tenían funciones divulgativas, se utilizaba para subir contenidos que no se podían modificar y solo eran para la consulta.

> […] la Web 2.0, en donde la red cambio a ser un medio colaborativo y de participación entre los usuarios, en el cual estos pueden generar cualquier tipo de contenido, difundirlo. Finalmente, la red además de ser colaborativa y participativa se movió a las redes sociales. Cuando la red fue participativa y colaborativa se volvió peligrosa para la estabilidad social, económica y política de la comunidad internacional (Carlini, 2018, p. 8).

Coincide con lo expuesto en precedencia respecto de la Web 2.0, Herreros (2008) al indicar que la mencionada web

> […] va más allá de la acepción técnica, o puramente instrumental, para profundizar en su dimensión comunicativa e informativa. No se entra en la descripción de su funcionamiento informático, sino que se pasa directamente a examinar el cambio producido en los procesos de interrelaciones de las personas o grupos sociales que intervienen en su aplicación, así como en las repercusiones que este enfoque tiene en la generación de un nuevo modelo comunicativo (Herreros, 2008, p. 346).

Agregó el citado autor que, con la incorporación de la web 2.0 las comunicaciones interactivas se expanden hacia nuevos modelos de redes sociales (Herreros, 2008, p. 253).

Asimismo, las redes sociales como herramienta inmersa en el ciberespacio no solo son utilizadas como un medio para entablar relaciones sociales, sino el lugar donde puedes además ejercer actividades comerciales, laborales y hasta educativas. Es decir, en las redes sociales se convirtió en una alternativa a los medios de comunicación tradicional, en la que y, por ello, se reúnen la red social como tal y los medios de comunicación (Gandasegui, 2011, p. 17).

Igualmente, citando a Mosquera (2018), estas relaciones mediadas por la tecnología, principalmente por Internet, son generadoras de cultura, la cibercultura, la cual se localiza en un espacio virtual o ciberespacio, sin tiempo cronológico ni territorio y habitado por cibernautas o internautas. Ese nuevo tejido social, esas nuevas estructuras que la sociedad ha ido moldeando a partir de la experiencia posmoderna y del consumo mediático, adquieren centralidad al momento de abordar el estudio de Internet como medio de masas (Mosquera, 2008).

El término redes sociales, según Costa y Piñeiro, quien cita a Cristakis y Fowler, las redes sociales son un conjunto organizado de personas formado por dos tipos de elementos: seres humanos y conexiones entre ellos (Cristakis y Fowler, 2010, p. 27), que configuran espacios de convivencia y conectividad definidos por medio de una serie de intercambios de carácter dinámico entre los sujetos que las forman (Costa & Piñeiro, 2012, p. 1460).

Por lo antes expuesto, las relaciones sociales se mueven simultáneamente entre las que se formaron en forma tradicional, es decir, en las cuales la interacción se efectuaba

en forma interpersonal, con contacto físico o visual fuera del ciberespacio y las que se construyen en la actualidad únicamente a través del uso de las herramientas tecnológicas, en las cuales además de compartir el espacio virtual, se basan en intereses, valores, generaciones y afinidades donde la rapidez, simultaneidad de la comunicación y la masividad son ejes claves de ellas (Cornejo & Tapia, 2011a, p. 223).

El ciberespacio permite que las relaciones sociales sean globales, transfronterizas, con identidad idiomática y hasta podría afirmarse que elimina las brechas sociales entre personas que tienen en común intereses, convicciones, ideales que convergen en un espacio virtual. Las redes sociales han venido a desvanecer barreras físicas, geográficas y sociales, permitiendo conectar a personas de todo el planeta. Esto constituye un logro de la tecnología, que permite que individuos que tengan un interés común, puedan darse, cita y conocerse en un espacio virtual. Así, las personas pueden estar conectadas sin importar su ubicación (Lampe, Ellison y Steinfield, 2006).

Ahora bien, las relaciones sociales creadas en el entorno del ciberespacio también presentan falencias, entre ellas, la privacidad y ausencia de confianza en la veracidad de la información que allí reposa, por cuanto no solo son utilizadas como un medio de información, elemento básico y transversal en toda relación social, que a la vez implica para quien lo posee el control y poder de ella (Gandasegui, 2011, p. 6). Además, la información puede ser utilizada como una amenaza a la intimidad personal que puede implicar la suplantación de identidad, ciberdelincuencia por mencionar algunos. Asimismo, el uso excesivo de la red social trae trastornos en el comportamiento, tales como aislamiento, pérdida de control en el tiempo de conexión, pérdida de tiempo laboral o académico, entre otros (Cornejo & Tapia, 2011, p. 227) situaciones ajenas a la presente investigación.

La información se torna el elemento preponderante en el uso de la red social y de las relaciones sociales desarrolladas en el ciberespacio, por tanto, esta resulta más importantes que el mismo software que soporta la red social, ya que las relaciones sociales y el número de ellas que se establezcan soporta la relevancia o no de la red social y su recordación en el entorno digital.

Otro punto es la veracidad de la información que soporta las relaciones sociales en el espacio virtual, debido a que el ciberespacio permite modificar su realidad física, económica, educativa, social y moral, aparentando una diferente, *rebosantes de virtudes y carentes de defectos*.

De manera que, el ciberespacio es un lugar de interacción para las relaciones sociales donde confluyen personas de diferentes edades, nacionalidades, ideas, razas, entre otras, lo cual motivó a que los estudiosos en el área. Aun cuando no hay claridad ni unanimidad sobre el origen de tales denominaciones, o como muchos le llaman, etiquetas, existen un conjunto de preceptos que gozan de mayor aceptación por el calificativo común, y es precisamente a ellos a los cuales se hará referencia.

Ahora bien, al referirse al término generación, este se encuentra definido por la Real Academia de la Lengua Española (RAE) como un conjunto de las personas que tienen aproximadamente la misma edad. La generación de nuestros padres. Conjunto de personas que, habiendo nacido en fechas próximas y recibido educación e influjos culturales y sociales semejantes, adoptan una actitud en cierto modo común en el ámbito del pensamiento o de la creación (La Real Academia de la Lengua Española, s.fb).

Para algunos autores, la edad no es el factor preponderante que define una generación, si no debe incluirse los acontecimientos históricos sociales que la rodean. Entre ellos, por ejemplo, encontramos a Kertzer (1983) quien la asocia con parentesco; con personas que tienen la misma edad y comparten momentos históricos, con etapas de la vida como la juventud, madurez o vejez, entre otras asociaciones (Díaz, Lopez y Roncallo, 2017, p. 193).

Otros la definen desde un punto de vista positivista, teniendo en cuenta el impacto social, modificación de su entorno o evolución social. También, existe una definición histórico-romántica en el cual la idea de generación son los hechos, circunstancias y acontecimientos que suceden en una época determinada o comparten un destino colectivo.

Cada una de las generaciones posee características propias que las diferencian, resaltando que las generaciones de los veteranos por su condición se encuentran gozando del retiro forzoso y no participan en forma activa en el uso de las herramientas tecnológicas.

La Generación Baby Boomers, su nombre, se debe al incremento de nacimiento ocasionado al terminar la Segunda Guerra Mundial. En su generación ocurrieron eventos de gran magnitud social, como son la expansión de la televisión en los hogares, el rock and roll, el primer hombre en la luna, el movimiento de los derechos civiles, los derechos de la mujer, el movimiento hippie, Woodstock y el asesinato de Kennedy (Díaz, López y Roncallo, 2017, p. 196).

Actualmente, se encuentran entre los 57 y los 75 años de edad que corresponde a una población activa en el área laboral y en cargos de poder, la cual se encuentra próxima a su retiro. Se caracterizan por su dedicación y hasta adicción al trabajo. Empoderados y esperando lo mejor de la vida, preocupados por la búsqueda de estatus, la lealtad y la calidad de vida (Díaz, López y Roncallo, 2017, p. 195). Es una generación que no creció con el internet, pero se adaptó a las herramientas tecnológicas y las usa como facilitares de su trabajo o vida personal. El aporte de ellos, es su experiencia y visión para la solución de problemas, buscan mediar ante cualquier conflicto, aunque prefieren laboral en forma individual y no colectiva.

La generación X o los nacidos entre 1961 a 1980. Actualmente, tienen entre 60 y 41 años, hijos de los Baby Boomers, padres de los Millennials y Centennials. Crecieron en

hogares donde ambos padres laboran o pertenecen a una familia disfuncional, ya sea porque sus padres se divorciaron o porque decidieron mantenerse solteros. Empoderados de su educación como herramienta de superación, vida digna y valiosa. Altamente consumistas, influenciados por el surgimiento de las computadoras personales, la expansión del internet, enfermedades como el VIH, la caída del muro de Berlín, surgimiento de canales de televisión por suscripción y especializados. Buscan un balance entre el trabajo y su vida personal. Adaptables a su entorno y al uso de las herramientas tecnológicas, pragmáticos, responsables y protectores con sus hijos (Díaz, López y Roncallo, 2017, p. 196).

La generación Y o Millennials, nacidos entre 1981 y 2004, hoy cuentan con edades que oscilan entre los 40 y 17 años, aunque se debe señalar que los autores no se ponen de acuerdo en el rango de fechas en las cuales oscila esta generación, principalmente por el inicio de la siguiente que es la Z o Centennials. Lo cierto es que son los hijos de los últimos Boomers y primeros de los X, crecieron con el uso de la tecnología como parte de su vida, ya que en 1981 IBM empezó a comercializar el primero ordenador, con el uso del internet, los teléfonos inteligentes, los avances tecnológicos, las redes sociales y la saturación de información por parte de los diversos medios de comunicaciones a los cuales tienen acceso por el uso de las herramientas tecnológicas.

Su generación fue impactada con eventos tales como el ataque del 11 de septiembre al World Trade center en el año 2001, la guerra de Irak y Afganistán, el tsunami de Asia, la recesión del 2008, el uso de plataformas de búsqueda, información como Google, Wikipedia, videos de YouTube, páginas sociales como Facebook, Twitter, entre otras.

Responden a un mundo globalizado y digitalizado, le dan importancia a la honestidad, la ecología, los productos orgánicos porque desean cambiar el mundo, el concepto de distancia no existe, ya que por el uso del ciberespacio viven experiencias multiculturales y se encuentran abiertos a nuevos retos. No tienen filiación política ni religiosa, el cambio es una constante en su entorno por lo que no guardan lealtad a sus empleadores, son por excelencia nómada. Sus hogares se encuentran formados por parejas activas laboralmente en donde la flexibilidad laboral es una de sus prioridades.

Finalmente, la generación de los Centennials, generación IGen o Z son los nacidos luego del 2005 en adelante, cuentan con aproximadamente 16 años o menos, son nativos digitales, rodeados de conectividad, computadores y teléfonos móviles, razones por las cuales son usuarios naturales y permanentes de las herramientas tecnológicas y el uso del ciberespacio en el cual acortan distancia mediante servidores. Satisfacen la mayor parte de sus necesidades básicas con el uso de apps, se comunican en forma constante y sin horario, prefieren ambientes de autoaprendizajes porque lo que necesitan aprender simplemente lo buscan navegando en el ciberespacio. Además, efectúan tareas múltiples y simultáneas, lo que los hace más competitivo, pero a su vez más distraídos, desconcentrados y con periodos cortos de atención.

La cultura de los Centennials se presentó como una gran diversidad de culturas locales que se conectan entre sí, las cuales se encuentran jerarquizadas por una estructura de poder a la que se agregan. En palabras de Krazov (2003), el modelo de estas culturas desterritorializadas sería el intercambio de bienes, informaciones, imágenes y conocimientos, patrocinado por redes de comunicación y dotado de cierta autonomía al nivel mundial (Jaramillo, 2018, p. 34). Lo que implica una simbiosis entre la cultura individual de cada país y la cultura colectiva construida en el entorno digital.

De modo que, la identificación de los valores de esas generaciones, así como sus luchas e ideologías inmersas en el ciberespacio se vuelven colectivas como parte de la problemática social de un país y globalizadas por su réplica en los demás miembros de esa colectividad geográfica ubicada en otro país.

Entonces, las generaciones Y y Z son las que más utilizan el ciberespacio como una herramienta de interacción social y política, no se puede desconocer que su uso depende del acceso que tenga de ella, lo que finalmente divide a la población y crea una brecha digital, que a su vez evidencia un indicador de desigualdad socioeconómica. Sin embargo, para esta investigación se parte del hecho del acceso en igualdad de condiciones a las herramientas tecnológicas.

Ahora bien, la participación social en el entorno digital se incrementa dependiendo no solo del acceso que se tenga a la herramienta digital, sino también al interés particular del participante internauta, con independencia de la generación en la cual se encuentra clasificado. Los mayores si bien no cuentan con la habilidad y experticia en el manejo y aprovechamiento del ciberespacio como lo tienen las generaciones Y y Z, lo cierto es que, se encuentra interesado en tener una participación social y políticamente activa con conocimiento e interés en la causa. En contraposición, los Millennials y Centennials nativos digitales pueden ser menos cautelosos respecto a su intervención en las diferentes clases de movimientos a los que son convocados.

Métodos de acercamiento y movilización de masas a través del ciberespacio.

La globalización trajo consigo la idea de romper y eliminar las fronteras –principalmente económicas– para facilitar la conexión entre sociedades, Internet ha vuelto posible, en todo caso, que la comunicación trascienda las fronteras del mundo real. Así, el empleo de las redes durante los últimos años ha elevado su nivel de incidencia en las dinámicas sociales, generando relaciones de afinidad que parten del conocimiento de los patrones con los que los internautas consumen información.

En palabras de Rihawi (2018) existen tres factores que describen las relaciones en el ciberespacio:

> Por un lado, la "-conectividad-", es decir, la capacidad que nos otorga la tecnología de transferir información tal y como hoy lo hacemos. Por otro lado, la "- interactividad-" se entiende la relación de las personas con el entorno digital a través de un hardware (todos los elementos instrumentales que son parte de la maquinaria de la computación, cables, torres, teclados, programas, periféricos, etc.) que les conecta a ambos. Y se debe añadir la "-hipertextualidad-", especialmente vinculada al trabajo que nos ocupa y que gira en torno a la posibilidad de la conexión interactiva con cualquier parte y en cualquier momento (Rihawi, 2013, p. 30).

Otra de las herramientas que ha facilitado la participación de las personas en el mundo virtual, se ha ejercido a partir del uso masivo de los teléfonos móviles inteligentes, a través de los que se tiene acceso a la información que se desprende desde el internet y por supuesto, de las redes sociales. Tal situación obedece a que los teléfonos móviles dieron el gran salto adelante en comunicabilidad y acercamiento de las personas a la comunicación y la información. Los teléfonos móviles son más baratos que los PC y el número de móvil triplicaban al de los ordenadores y su penetración crece al doble de la velocidad de estos y cada vez son más los que incorporan acceso a Internet (Rihawi, 2013. P.50).

Las redes sociales son medios, donde las personas pueden crear perfiles bien sean reales o que se desprendan de un imaginario que pocas personas pueden corroborar, favoreciendo así, la distribución de información con la que pueden o no sentirse cómodos ante las personas de su entorno físico, pero que podría variar con su interacción en la red.

Las nuevas relaciones en la red despertaron en la sociedad la creación de nuevas interacciones políticas donde la motivación, la conjugación del internet, los teléfonos celulares y las motivaciones de gremios, movimientos políticos y vertientes sociales aumentaron su incidencia en la red con el objetivo de ganar seguidores, compartir información, seguir las comunicaciones y generar suscripciones, motivados por la facilidad de llegar en tiempo real a cualquier audiencia.

En estos movimientos sociales se hizo hincapié en la importancia de las redes sociales como elemento aglutinador, disparador, motivador, conductor y herramienta usada para la gestión y proyección de activismo, como, además, se ve desde la perspectiva de una de las redes que más ha influido últimamente, nos referimos a Twitter (Rihawi, 2013; ello, teniendo en cuenta que es una red a través de la que se permiten generar posturas de opinión sea compartida y difundida sin limitaciones.

Se ha democratizado la información y de alguna manera ya no se debe esperar a que nos cuenten las cosas. Las personas ya buscan y eligen las respuestas que necesitan, pudiendo tener varios puntos de vista del mismo fenómeno social y, por lo tanto, sacar unas conclusiones más claras de lo que sea. Ya se comienza a establecer la idea que la información también puede ser emitida por el que era su receptor tradicional, el gran público (Rihawi. 2013.p. 51).

Uno de los hechos históricos que dan cuenta de ello, se puede observar con los sucesos ocurridos en la primavera árabe en la que "estallaron una serie de revueltas en varios países árabes y provocaron la caída de regímenes que llevaban décadas en el poder, en algunos casos de una forma increíblemente rápida" (Soengas. 2013. P. 148), lo cual, sin duda, construyó patrones de comportamiento humano que moldearon nuevas dinámicas de relación entre las personas, debido a que ante la constante presión política que se ejercía mediante la coerción, esta perdió relevancia en la medida en la que las personas podían interactuar y emitir sus posturas de oposición, sin poner directamente su vida en riesgo.

En este punto, resulta necesario diferenciar que existen tres tipos de redes sociales (Celaya, r2008) a saber: Redes profesionales (por ejemplo, LinkedIn, Xing, Viadeo), Redes generalistas (por ejemplo, MySpace, Facebook, Instagram, Hi5) y Redes especializadas (por ejemplo, Ediciona, eBuga, CinemaVIP, 11870) (Hütt, 2012, p. 123). El primer tipo de red se caracteriza por permitir el "Networkig" que es un círculo social-profesional que brinda oportunidades de crecimiento para tu empresa, en el cual se cuenta con una lista de contactos profesionales tanto para intercambios mercantiles como para establecer relaciones sociales y oportunidades de empleo. Por lo general, cuando haces parte de la red social subes tu hoja de vida, se cuenta con un buscador interno y se crean grupos por perfiles profesionales o comerciales.

En el segundo tipo de red social, esta es, la generalista, los perfiles de los usuarios son comunes, participan todo tipo de individuos sin limitaciones de edad, sexo, intereses o ámbito cultural, los contactos se generan por búsqueda personalizada y se comparte información de ocio. Los perfiles pueden ser o no reales, por lo que el control de saber con quién estás relacionado es casi nulo (Hütt, 2012, p. 124).

Y finalmente, en las redes sociales especializadas se refiere a una determinada actividad social o económica, deporte o materia, motivos por los cuales, los seguidores se basan en los gustos o preferencias, como por ejemplo Flixster que es una red social de los amantes del cine.

Ahora bien, los métodos de acercamiento con los cibernautas también dependen del tipo de rede social que se esté desarrollando, por cuanto, si es una red profesional, el tipo de cuenta será corporativo y, por tanto, se crean espacios de promoción, información, mercadeo a los cuales se les hace un proceso de seguimiento y mejora continua. Si es una red social generalista, el acercamiento con los cibernautas de manera primigenia se efectúa a través de sus conocidos, léase, familia, amigos del colegio, de estudios técnicos, tecnológicos, profesionales, especializados o por elección de preferencias en actividades de ocio.

Esos mismos contactos se encargan de ampliar la red. Cuando los cibernautas se organizan y forman un movimiento de masas con un objetivo común, se forma un

colectivo informal como un tipo de movimiento social no tradicional conocido como el *Smart mobs* con una agenda amplia que puede ir desde asuntos como los derechos humanos, la ecología, los valores culturales o expresiones de inconformismo en contra de una determinada acción del Estado, eliminando las jerarquías y la representación indirecta de sus intereses.

Los *Smarts mobs* efectúan convocatorias colectivas mediante el envío de mensajes en cadena para lograr el movimiento de masas (Candón, 2021, p. 15), en la mayoría de los casos son anónimas para evitar conflictos de identificación con una persona o grupo determinado. Aunque detrás de dicha convocatoria existen reuniones preparativas, determinación del recorrido de la marcha, su legalización, redacción de un lema, fecha y lugar. La llamada al movimiento de masas debe ser atractiva, sugestiva y debe verse masiva. Las cadenas de mensajes a la movilización son una forma de organizarse sin organización.

Esa cadena de mensajes no solo fue enviada por medio de mensajes de texto, sino también utilizando redes sociales como Twitter, Facebook, Telegram, por mencionar algunas, con la información precisa de la convocatoria citada en precedencia. Dicha información a su vez fue reenviada por los miembros a sus propias redes o grupos sociales virtuales a los que pertenecen, lo cual produce un efecto dinámico y masivo que demuestra el éxito de acercamiento.

Asimismo, al interior del colectivo las diferentes redes sociales se utilizan en forma diversa, es decir, no solo se convoca, sino que además se sube contenido, videos en Youtube, Instagram, Telegram o Signal. Para obtener recordación y masificación, las etiquetas en los Twits deben ser mencionadas por otros seguidores. El impacto de la movilización de masas a través del ciberespacio se obtiene con la recordación, con la información constante y al momento de la forma en que se desarrolla y la retroalimentación de las decisiones a tomar para obtener la meta trazada.

Por ejemplo, en el movimiento español 15M la forma como se enteró el público de la movilización de masas fue por medio de redes sociales como Facebook, Twitter, SMS, correos, la manifestación misma, entre otros (Domínguez et al., 2019, p. 1264).

En Colombia, para el movimiento 21N, de acuerdo con Rodríguez Rojas, la red social que más tuvo actividad fue el twitter, tanto cuentas oficiales como las del Presidente Iván Duque, congresistas y expresidentes, como cuentas de influenciadores de oposición, así como cuentas de medios de comunicación y comunidades de opinión (Rodríguez, 2020, p. 18). Para el paro nacional del año 2021 el método de acercamiento para la movilización de masas tanto nacional como internacional también fueron las redes sociales. Por ejemplo, el día del inicio del Paro Nacional (28 de abril), en latitudes como Madrid, Berlín, Minnesota, Melbourne, entre otros, se presentaron manifestaciones de apoyo y solidaridad (Roa, 2021, p. 204).

En Nueva York, Catalina Cruz, que representa al Distrito 39 en la Asamblea de ese Estado, fue una de las gestoras de las marchas en esta ciudad (Roa, 2021, p. 206).

Asimismo, en Facebook se crearon comunidades de colombianos o con la identificación de Paro Nacional, igual sucedió con Twitter, Telegram y Youtube que fueron utilizados para efectuar las convocatorias a las movilizaciones, así como divulgar información simultánea, sucesiva y en tiempo real de los bloqueos, enfrentamientos, desmanes entre otros. La red social de Telegram y Signal fue utilizada no solo para lo citado en forma previa, sino además para dar instrucciones de cómo defenderse en caso de ser objetos de ataques por parte de la fuerza pública, tanto en su integridad física como legal, como atacar a los vehículos utilizados por los agentes del Estado para contener la protesta no pacífica entre otras cosas.

En ese sentido, las redes sociales virtuales son el medio idóneo para llevar a cabo la movilización de masas, en la cual convergen diferentes actores, por una parte, las cuentas estatales o que representan al Estado, los de la oposición y la comunidad organizada en los diferentes espacios virtuales. A través de ellas, se convocó, mostró, informó, instruyó y denunció en forma permanente y coetánea tanto la problemática social que disparó el movimiento de masas como su transcender diario.

Efectos de la movilización de masas a través de ciberespacio en el orden público.

En la actualidad la movilización de masas que utiliza como herramienta de comunicación el uso de internet, se denomina crowd, el cual significa en forma literal multitud. No es solo la suma de muchas personas, sino que es entendido como una comunidad que se comporta de una manera determinada. Con el nacimiento de redes sociales como Twitter o Facebook, el crowd acuño el término de multitudes inteligentes (Gil, 2017)

Parafraseando a Rheingod (2002), el poder de la multitud se observa en la capacidad de superar las restricciones físicas de la planificación urbana, así como esfumar las distinciones sociales. Su autoridad reside en la capacidad de fomentar el movimiento y la agitación. Se puede definir como una especie de tecnología en sí misma y no simplemente como una reunión de personas a través de los sistemas tecnológicos (Gil, 2017).

En ese sentido, las masas sociales que interactúan en el ciberespacio son entes sociales activos que construyen su propia realidad. Su ciberactivismo puede pasar de simplemente manifestaciones culturales o de moda a tener un impacto social y político.

Cuando el uso del ciberespacio pasa de ser ocioso, es decir, de compartir archivos con contenidos musicales, audiovisuales y programas informáticos a compartir en forma explícita contenido político, información con sentido crítico, efectuar convocatorias y

maquinar estrategias de intervención política, social y económica se crea una generación con valores de red, como la libertad de información.

Un ejemplo de los efectos de la movilización de masas a través de ciberespacio en el orden público a nivel internacional fueron los acontecimientos ocurridos en el año 2011 a nivel mundial, en los cuales se generaron conciencias colectivas a través de las redes sociales y digitales, convirtiendo el mencionado sitio en un lugar de conspiración y difusión de una crítica social transversal y masiva a los sistemas de poder que regían en el momento, responsables de cambios y crisis.

Como primer ejemplo se tiene lo ocurrido en la primavera árabe de 2011 que provocó la caída de regímenes que llevaban décadas en el poder. Los detonantes del conflicto en Túnez, Egipto y Libia fueron las grandes diferencias sociales, la corrupción política, el abuso del poder, la falta de libertad y represiones continuas, restricciones de los derechos básicos de los ciudadanos, ostentación y privilegios de los gobernantes, etc. (Rihawi, 2017).

Los jóvenes árabes, teniendo en cuenta que los medios de comunicación oficial eran manejados por los Estados, utilizaron el ciberespacio como medio para ejercer su libertad de información, de expresión, de opinión y de asociación, demostrando la realidad que estaban viviendo y provocando una lucha para obtener un cambio político integral. Las ciber convocatorias por la lucha congregó miles de ciudadanos que se concentraron en la plaza Tahir e hicieron que la problemática a nivel internacional fuera visible, lo que, finalmente, implicó la modificación del régimen.

En Colombia, los efectos de la movilización de masas a través del ciberespacio afectó el orden público, por cuanto ha implicado la destrucción de la propiedad privada o pública, disturbios y acciones violentas protagonizadas por los manifestantes y en algunas ocasiones por las autoridades públicas, por mencionar algunas.

En el marco de la movilización de masas como expresión del ejercicio derecho a la protesta social, resulta necesario indicar que en Colombia se encuentra garantizado su ejercicio en la Constitución Política en su artículo 20, el cual establece que: se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación (Congreso de la República de Colombia, 1991).

Asimismo, el artículo 37 se señala que toda parte del pueblo puede reunirse y manifestarse pública y pacíficamente y la ley podrá establecer de manera expresa los casos en los cuales se podrá limitar el ejercicio de este derecho (Congreso de la República de Colombia, 1991) y finalmente, el artículo 56 se dispone que se garantiza el derecho de huelga, salvo en los servicios públicos esenciales definidos por el legislador (Congreso de la República de Colombia, 1991).

Sumado a lo señalado, el mencionado derecho no es ilimitado, se encuentra restringido por un pronunciamiento de la Corte Constitucional que en sentencia C- 122 de 2012 por el interés general, los derechos de los demás y cuando su ejercicio suponga la alteración del orden público, por lo que, el derecho a la protesta está permitido cuando sean afectados intereses generales.

Adicionalmente, el Código Nacional de Policía y Convivencia reguló en varios de sus artículos la protesta social que es ejercida en el espacio. Solo por mencionar algún ejemplo, la mencionada norma indica que:

> Toda persona puede reunirse y manifestarse en sitio público con el fin de exponer ideas e intereses colectivos de carácter cultural, político, económico, religioso, social o de cualquier otro fin legítimo. Con tales fines debe darse aviso por escrito presentado ante la primera autoridad administrativa del lugar o mediante un correo electrónico. Tal comunicación o correo debe ser suscrito por lo menos por tres personas y deberá expresar día, hora y sitio de la proyectada reunión y se presentará con 48 horas de anticipación indicando el recorrido proyectado. Toda reunión y manifestación que cause alteraciones a la convivencia podrá ser disuelta (Congreso de la República de Colombia, 2016, párrafo 22).

En ese sentido, es claro que la protesta social es permitida en Colombia con unos fines legítimos, aunque no se define cuáles sean, ni los criterios con los cuales se establecen. No se permiten las manifestaciones espontáneas por cuanto se debe surtir el aviso a la autoridad mencionado líneas atrás.

Desde el punto de vista penal Código Penal Colombiano (2000) esto es, el reproche social y tipificado en la ley por el ejercicio de la protesta no pacifica, normalmente implica tres delitos de acuerdo con la Ley penal colombiana, estos son: Asonada, perturbación en servicio de transporte público oficial y obstrucción de vías públicas.

En principio, la convocatoria a la movilización de masas es pacífica, pero al transcurrir del tiempo y observar que no se obtiene el resultado deseado o es no efectiva se torna violenta y comienza el enfrentamiento con los agentes del Estado.

En este punto, es necesario indicar que en ocasiones la movilización de masas como manifestación de la incomodidad ciudadana resulta cotidiana, motivo por el cual, no es efectiva y no se modifica el statu que objetivo de ella. Para gozar de esa cotidianidad, los medios de comunicación juegan un papel preponderante porque informar en forma diaria noticias con contenido negativo o relacionado con ese malestar hace que el pueblo se acostumbre a tal circunstancia y, por tanto, no vea necesario participar en la movilización generando un ambiente de apatía a la causa.

Ahora bien, si la protesta es considerada legítima, puede ser eficaz. Sin olvidar que aquella siempre debe ser pacífica, por cuanto, en el momento que se vuelca violenta, puede perder simpatizantes y credibilidad tanto por la causa como por sus participantes. Aclarando que no siempre coinciden el participante con el delincuente o aquel que ejerce

su derecho de protesta en forma violenta. Desde el punto de vista del Estado y, bajo el mismo concepto del derecho a la protesta, la violencia no es el medio adecuado para obtener el cambio social deseado. Hoy el ciberespacio es el medio ideal para ejercer la democracia en una sociedad virtual.

Una de las formas legítimas con las cuales cuenta el Estado para controlar los disturbios generados por un movimiento de masas ejercido por medios violentos, es creando leyes o normas que restrinjan su actuar. En Colombia, la Ley 1801 de 2016, limitó el momento, la razón y la forma en la cual se puede efectuar una protesta social que se considere legítima y establece las sanciones cuando tales condiciones son quebrantadas (Congreso de la República de Colombia, 2016). Tal forma de control tiene sus fanáticos y sus detractores. Los primeros, la apoyan por ser un medio no violento para controlar el desborde de la protesta social; los segundos la ven como un instrumento para desestimular el derecho constitucional con el garrote de la conducta penal.

Otro mecanismo para controlar los disturbios en la protesta social es el aumento del pie de fuerza policial, que trae en forma inminente la disolución de las revueltas, aunque ello implica el uso de la fuerza y en casos aislados su exceso, lo que a su vez trae una respuesta negativa y violenta de los participantes y, por tanto, un círculo vicioso de uso de la fuerza entre los agentes del Estado y estos.

Como réplica a dicho mecanismo de control estatal, los participantes del movimiento de masas ven en el ciberespacio el medio idóneo y eficaz para contrarrestarlos. Por eso, el uso de las redes sociales como Telegram, WhatsApp, Instagram, Facebook, entre otros, se volvió el escenario perfecto anónimo para los participantes y gestores de la protesta social para organizarse, atraer adeptos y hacer visibles su malestar. En muchas ocasiones, mostrando en forma sesgada o parcializada los enfrentamientos entre los agentes del Estado y los manifestantes.

Desde noviembre de 2019 se efectuaron en varias ciudades de Colombia como Bogotá, Cali, Medellín, Tunja, Ibagué, Manizales, Armenia, Popayán, entre otras, movimientos de masas, esto es, paro nacional en contra del llamado *paquetazo neoliberal* que comprendía las reformas tributaria, pensional y laboral, aunado al descontento por el incumplimiento de los acuerdos de paz, el asesinato de líderes sociales y reinsertados, la privatización de empresas estatales, la corrupción, entre otros. Quien dirigió el paro nacional en principios fueron las centrales obreras a las cuales se le unió organizaciones sindicales, estudiantiles, sociales y políticas.

Todo lo precedente dio nacimiento al movimiento social denominado 21N, el cual tuvo auge en las redes sociales y tuvo como efecto la paralización del país, el cerramiento de empresas y establecimientos de comercio. A esta manifestación le siguieron la de los días precedentes 22N, 23N, 27N, 4D y 8D, es decir, se extendió entre los meses de

noviembre de 2019 a enero de 2020. Una de las características del citado movimiento fue la participación activa de jóvenes a lo largo del país, quienes utilizaron su creatividad para hacer del movimiento de masas toda una festividad.

La acción colectiva juvenil de la protesta social se caracterizó por la comunicación, la confianza, la colaboración y la construcción de lo común que se exteriorizó por medio de los cacerolazos y las batucadas

Definidas como ritmos repetitivos interpretados por un grupo de personas que busca *romper con el orden y los rituales de la política callejera*, generando un impacto comunicativo por su musicalidad y puesta en escena que hace que tanto participantes como transeúntes sientan, vibren y rían con sus letras (Aguilar-Forero, 2020).

Con posterioridad a los cacerolazos, sobrevino una campaña de miedo, la cual de acuerdo con Aguilar-Forero (2020) fue una medida de control ejercida sobre la población para desmotivarla a participación y luego se convirtió en un miedo paranoico según el cual delincuentes ingresaban a los conjuntos residenciales a destrozarlos, lo que implicó que los residentes se organizaran y se armaran para defender su propiedad privada poco antes de decretar un toque de queda.

Otra de las acciones llevadas a cabo en el paro nacional fue el denominado *primera línea*, esto es, jóvenes con escudos azules ubicados en el frente de las marchas organizados e instruidos en el evento de ser heridos por el personal de la policía o ser detenidos por su participación violenta.

El 21N y sus sucesores fueron apoyados por varios sectores de la población civil y la guardia indígena, quienes crearon barreras alrededor de los manifestantes con el fin de evitar desmanes a los establecimientos públicos o privados e inclusive contra la fuerza pública. Todos estos movimientos, al parecer sin líder identificable, dieron nacimiento a un grupo dirigente llamado *Comité del Paro*, en los cuales participaron dirigentes de las centrales obreras y jóvenes estudiantes, entre los cuales surgió la pregunta de a ¿Quién representa a quién? Y ¿Quién hablan por quién?, finalmente, los estudiantes tomaron la vocería.

Como consecuencia de la declaración de la pandemia por el virus Covid-19 los movimientos sociales tuvieron un cese de actividades, las cuales fueron reactivadas en el año 2021, exactamente el día 28 de abril con el lema *Por la vida, la paz, la democracia y contra la Reforma Tributaria y el paquetazo de Duque* establecida por el Comité Nacional de Paro, retomando las exigencias relacionadas con el retiro de la reforma tributaria, cumplimiento de acuerdos previos, educación entre otros.

Todas estas redes sociales virtuales fueron la herramienta del crowd para ejercer su protesta social y obtener que la mencionada reforma tributaria presentada por el gobierno nacional fuera retirada. No obstante, al haber obtenido su objetivo, el movimiento

social permaneció y retomó las metas con las que se habían iniciado el 21N, entre las que se puede contar el retiro de la reforma a la salud, la gratuidad de la educación universitaria, el cumplimiento de acuerdos previos con los educadores e indígenas. Todas estas razones hicieron que el Paro Nacional y sus participantes permanecieran por varios días, con las implicaciones económicas y sociales negativas para el pueblo, como fueron el incremento en el valor de los productos de la canasta básica, la destrucción de bienes privados y públicos, el sistema integrado de transporte publicó, la quema de varios puestos de policía e inclusive el lanzamiento de bombas incendiarias contra los miembros de la policía que culminó con actos atroces como la quema viva de algunos de ellos.

En la medida que el exceso de la fuerza de los participantes del movimiento de masas creció, el uso de la fuerza para neutralizar las acciones violentas se hizo más evidente por las constantes agresiones físicas y verbales a los que fueron sometidos los agentes del Estado, lo cual ocasionó desmanes de lado y lado. Como respuesta, los ciber participantes de los grupos sociales mencionados crearon manuales de primeros auxilios médicos, manejo de miedo y primeros auxilios legales, todos los cuales fueron difundidos por medio de la red.

Cabe mencionar que a la protesta social y debido a los infortunios, decesos, lesionados, caos, daños físicos a la propiedad privada y pública, a dichos grupos sociales liderados por supuestos jóvenes inconformes, bajo el lema, se metieron con la generación que no tiene miedo se unieron jóvenes profesionales o finalizando sus carreras de medicina, derecho y comunicación para ayudar a quienes estaban enfrentando y participantes en forma directa en la protesta, los denominados primera línea con el fin de prestarles y organizarlos desde el punto de vista legal, físico, suministros, salud, entre otros.

Incluso, en las redes sociales debido al grado de violencia en el que se convirtió el ejercicio del derecho a la protesta y, con el fin de salvaguardar responsabilidades y hacer visible a nivel internacional el malestar de los participantes, se emitieron instrucciones en forma de manual de seguridad digital, en el cual no solo se explicaba el manejo del teléfono inteligente, sino además, las seguridades que debían tomar para participar en forma anónima en la red utilizando una VPN, como subir videos con indicación geo referencial de donde se encontraba el participante y evitar ser rastreados por los analistas de seguridad del Estado.

Otra de las redes sociales virtuales utilizadas en Colombia para efectuar la protesta social fue Twitter bajo los hashtags #SOSColombiaDDHH, #SOSColombia #Nosestanmatando, entre otros, en los cuales se denunciaba que las redes sociales utilizadas por los manifestantes para desestabilizar el orden público en diferentes partes de Colombia habían sido intervenidas por agentes del Estado para impedir que el mundo viera lo que en realidad le estaba sucediendo al pueblo. Se subieron imágenes de enfrentamientos entre la fuerza policial y los manifestantes, así como se buscaron personas que presuntamente estaban desaparecidas.

Todo lo precedente demuestra que entre los efectos principales del movimiento de masas a través del ciberespacio en el orden público es desestabilizar el país a través del caos, la destrucción y el vandalismo. Aunado a la desinformación o información parcializada en contra de los agentes del Estado, incomunicación entre las diferentes regiones del país y hasta en la misma ciudad, lo que ocasionó a su vez el desabastecimiento de comida, aumento de precios, perdida de producción y elevado endeudamiento.

Conclusiones

El ciberespacio es el nuevo espacio de construcción de relaciones sociales, es el medio donde se ejerce el ser social propio de la naturaleza humana. Las relaciones sociales modernas alternan y confluyen entre el espacio físico y el virtual, en el cual la conectividad de los dispositivos móviles se configura como el eje de las relaciones sociales.

El espacio virtual actual donde se establecen relaciones sociales se denomina redes sociales virtuales, la web paso de ser instrumental a incluir las dimensiones comunicativas, informativas e interactivas. Este proceso dio el nacimiento a la cibercultura ejercida por un cibernauta en un espacio sin territorio, sin tiempo, multilingüal, multirracial, sin brechas sociales, en donde se comparten intereses, valores generacionales en donde la rapidez, simultaneidad de la comunicación y la masividad de ella son sus ejes. Allí se entablan relaciones comerciales, laborales, educativas y de ocio.

El uso del ciberespacio depende de la generación a la cual pertenezcas, el interés que te mueva y el acceso que puedas tener. Este último genera crea una brecha en el empleo de las tecnologías. Las generaciones que más interactúa en el espacio virtual son los Millennials y los Centennials primigenios en ser digitales, innatos en el uso de las tecnologías disruptivas y saturadas de información.

En la virtualidad y las relaciones sociales se experimenta, se relaciona, se comunica y se conoce, en otras palabras, se efectúan procesos de acceso, divulgación y tratamiento de información, lo cual se traduce en conectividad, interactividad e hipertextualidad, todo lo cual se ha vuelto masivo gracias al empleo de los teléfonos móviles.

Las aplicaciones propias de los teléfonos móviles han permitido el intercambio de información por medio del uso del correo electrónico, videos a través de YouTube, simpatizantes utilizados los blogs, Twitter o las redes sociales como Facebook, Instagram y el intercambio de mensajes en WhatsApp, Telegram entre otros, cuyo origen puede provenir de perfiles reales o no en los cuales se publica el sentir o la filiación político social de quien publica, agradable o no para sus seguidores.

El ciberactivismo provoca el surgimiento de líderes quienes coordinan el grupo o red social virtual, cuyos miembros se encargan a su vez de replicar y ampliar su radio de

acción e impacto social, formando una inteligencia colectiva en la cual comparten información, construyen, crean, comparten, debaten, sugieren y convocan.

Las redes sociales virtuales constituyen el aglutinador del activismo social de la proyección y gestión de proyectos o movimientos sociales en pro de una causa en común. Los cibernautas buscan información, eligen las respuestas que necesitan dependiendo de su elección social, político y económica, por lo que el origen de la información se encuentra en el receptor tradicional, esto es, el gran público.

La participación ciudadana no solo evolucionó en la inteligencia colectiva, sino que sumo los sentimientos de afinidad, pasión e identificación de valores como la justicia, la verdad, la reparación que traspasaron al mundo virtual y dieron nacimientos a movimientos sociales como la primavera árabe y el 15M en España, todos se fundamentaron en la inconformidad por alguna condición social, económica, política interna o externa.

La autoridad del crowd (multitud inteligente) radica en la capacidad de fomentar el movimiento y la agitación social. Es una tecnología en sí misma, con su propia realidad.

En Colombia, la disconformidad social se reforzó en el año 2019 con el movimiento 21N que se extendió hasta enero de 2020 y luego se reactivó en abril de 2021 con el anuncio por parte del Gobierno Nacional de la reforma tributaria, lo que ocasionó un movimiento social virtual que impacto en forma negativa en la economía, en la vulneración de la propiedad privada o pública, disturbios y acciones violentas propiciadas por los manifestantes en contra de las autoridades públicas.

Una manera de controlar al movimiento de masas que se torne violente es por medio de la expedición de leyes y el aumento de pie de fuerza policial.

En Colombia el movimiento social virtual del año 2021 convocado por medio de las redes sociales, entre ellas, Telegram se denominó t.me/ParoNacional, t.me/ParoIdenfindo, @viva_el_paro_nacional en donde los participantes no solo fueron convocados a cesar actividades y obstruir la movilidad, sino, además, se dictaron instrucciones de la forma de aplacar la fuerza policiaca, defenderse en caso de detención, de prestar primeros auxilios y hasta ayuda legal en el evento de detención.

El efecto principal del movimiento social efectuado a través del ciberespacio en el orden público es la desinformación o información parcializada, el vandalismo, caos, la incomunicación territorial, fomentada a partir de la creación de identidades, pasionalismos y sentidos de pertinencia.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con el artículo. Se debe declarar el nombre del proyecto de investigación, grupo de investigación y organización a la que pertenece.

Declaración de divulgación

Diego Fernando Benjumea Gutiérrez. Magister en Escuela Superior de Guerra General "Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia.

ORCID: https://orcid.org/0009-0002-5805-2834
Contacto: benjumead@esdeg.edu.co

Referencias

Aguilar-Forero, N. (2020). Las cuatro co de la acción colectiva juvenil: el caso del paro nacional

Candón, J. (2021). U*sos de Internet para la organización de los movimientos*. https://core.ac.uk/download/pdf/51390134.pdf

Lampe, C., Ellison, N. and Steinfield, C., (2006). A *Face(book) in the Crowd: Social Searching vs. Social Browsing. In Proceedings of the 2006 20th Anniversary Conference on Computer-Supported Cooperative Work (CSCW 2006)*. ACM Press.

Cárcamo, H. (2005). Hermenéutica y Análisis Cualitativo. *Cinta de Moebio*, (23). https://www.redalyc.org/pdf/101/10102306.pdf

Cardi, A. (2018). *La redes sociales como factor de desestabilización*. Instituto Español de Estudios Estratégicos.

Carlini, A. (2018). *Las redes sociales como factor de desestabilización*. Boletín Instituto Español de Estudios Estratégicos, 11, 216–230.

Castañeda, L. (2010). *Aprendizaje con redes sociales. Tejidos educativos para los nuevos entornos. 1er edición*. https://www.academia.edu/311747/Aprendizaje_con_redes_sociales_Tejidos_educativos_para_los_nuevos_entornos

Christakis, N. A. & Fowler, J. H. (2010). *Conectados*. Taurus.

Congreso de la República de Colombia. (1991). *Constitución Política de Colombia*. https://d1wqtxts1xzle7.cloudfront.net/55690712/Constitucion_politica_de_Colombia_-_2015-with-cover-page-v2.pdf

Congreso de la República de Colombia. (2000). *Colombia Código Penal*. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Congreso de la República de Colombia. (2016). Ley 1801 de 2016 *Código Nacional de Seguridad y Convivencia Ciudadana*. https://bibliotecadigital.ccb.org.co/handle/11520/24704

Cornejo, M., & Tapia, M. L. (2011). Redes sociales y relaciones interpersonales en internet. *Fundamentos en Humanidades*, 13(24), 219-229. https://www.redalyc.org/pdf/184/18426920010.pdf

Costa Sánchez, C., & Piñeiro Otero, T. (2012). Activismo social en la web 2.0. El movimiento 15M. Vivat Academia, (117), 1458-1467.

Domínguez, D. C., Terceño, J. R., & Barrientos, A. (2019). El malestar social a través de las nuevas tecnologías: Twitter como herramienta política. Revista latina de comunicación social, 74, 1264–1290.

Ghiso, A. (1996). Métodos de la investigación cualitativa. Ediciones Aljibe.

Gibson, W. (1984). Neuromancer. Editorial Ace.

González, P. (2013). La hermenéutica y el método de la ciencias sociales. Cuadernos de Filosofía Latinoamericana, 34 (109).

Grossetti, M. (2009). ¿Qué es una relación social? Un conjunto de mediaciones diádicas. Redes *Revista hispana para el análisis de redes sociales*, 16(1), 44.

Kertzer, D. I. (1983). Generation as a sociological problem. *Annual review of sociology, 9*(1), 125-149.

Krazov, E. (2003). Globalización e identidad cultural. *Revista Mexicana de Ciencias Políticas y Sociales*, 237–245.

Díaz, S. C., López, L. M. y Roncallo, L. L. (2017). Entendiendo las generaciones: una revisión del concepto, clasificación y características distintivas de los Baby Boomers, X Y Millennials. *Clío América*, 11(22), 188 - 204.

Herreros, M. C. (2008). La Web 2.0 como red social de comunicación e información. E*studios sobre el mensaje periodístico,* 14, 345–361.

Hütt Herrera, H., (2012). Las redes sociales: una nueva herramienta de difusión. Reflexiones, 91(2), 121-128.

La Real Academia de la Lengua Española. (s.f). Relación. https://dle.rae.es/relaci%C3%B3n

La Real Academia de la Lengua Española. (s.fb). Generación. https://dle.rae.es/generaci%C3%B3n

Mosquera Villegas, M. A. (2008). De la Etnografía antropológica a la Etnografía virtual. Estudio de las relaciones sociales mediadas por Internet. *Revista Venezolana de Sociología y Antropología,* 18(53), 532-549 https://www.redalyc.org/pdf/705/70517572006.pdf

Orihuela, J. L. (2008). *Internet: la hora de las redes sociales*. Unav.edu. https://dadun.unav.edu/bitstream/10171/2962/1/nueva_revista_08.pdf

Paro Nacional #28 abril no a la reforma tributaria. (2021). *Facebook.com*. https://www.facebook.com/groups/548019452410213/?ref=share

Pérez, D. (2015). Hacia dónde va la movilización social. *El Siglo del Gorreón*. https://www.elsiglodetorreon.com.mx/noticia/2015/hacia-donde-va-la-movilizacion-social.html

Pinzón Flórez, N. L. (2014). *Caracterización del ciberactivismo en Facebook en el marco del proceso electoral* [Universidad Tecnológica de Pereira.]. https://core.ac.uk/download/pdf/71398703.pdf

Riaño, L. (2018). Movimientos sociales herramientas conceptuales *Revista de Estudios Políticos y Estratégicos*. 6(2), 36-57.

Rihawi Pérez, N. (2017). El papel de las redes sociales en la cibercultura: el caso de la "primavera árabe". Universidad Complutense de Madrid. https://eprints.ucm.es/id/eprint/47935/

Roa, M. G. (2021). *Lejos, pero no ausentes. movilizaciones diaspóricas en el paro nacional del 2021*. https://www.researchgate.net/profile/Jan-Grill/publication.

Rodríguez Rojas, S. A. (2020). #Paro21denoviembre: un análisis de redes sociales sobre las interacciones y protagonistas de la actividad política en Twitter. *Análisis Político*, 33(98), 44–65.

Soengas-Pérez, X. (2013). El papel de Internet y de las redes sociales en las revueltas árabes: una alternativa a la censura de la prensa oficial. *Comunicar,* 21(41), 147–155.

Jaramillo, M. (2018). A*daptación de gestión humana para recibir a la generación z (centennials) en las grandes empresas del Valle de Aburrá* [Trabajo de Grado]. Universidad EIA Ingeniería Administrativa Envigado.

Rihawi Pérez, N. (2018). *El papel de las redes sociales en la cibercultura: el caso de la "primavera árabe"*[-Tesis doctoral]. Universidad Complutense de Madrid.

Gil, M. (2017). Nuevos activismos sociales en la era digital: de las masas al crowd. Polít. Soc. (Madr.), 54(1) 191-208.

Rheingold, H. (2002). *Multitudes inteligentes: la próxima revolución social (Smart Mobs)*. Gedisa.

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 1, número 2, julio-diciembre 2022 (pp. 167-178)
Bogotá, D.C, Colombia

EDITORIAL **ESDEG**

El Ciberespacio como escenario para enfrentar los delitos transnacionales en Colombia

Cyberspace as a scenario to confront transnational crimes in Colombia

DOI: https://doi.org/10.25062/2955-0270.4769

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

Resumen

El presente artículo de contexto permite realizar un acercamiento a la importancia de identificar el ciberespacio como medio utilizado por las organizaciones criminales transnacionales, para la materialización de sus delitos de manera efectiva y segura. De la misma forma se aborda el papel determinante que juega el ciberespacio como dominio transversal a los dominios físicos de la guerra, siendo incluso nombrado en varios países como el quinto dominio que desarrolla un papel fundamental en la lucha contra los delitos trasnacionales. Finalmente, se formularon algunas estrategias que con una sinergia institucional seguirán sumando esfuerzos en las luchas contra los flagelos de la delincuencia transnacional en Colombia.

Palabras Clave: Ciberespacio; Delitos; Dominio; Información.

Abstract

This context article allows us to approach the importance of identifying cyberspace as a means used by transnational criminal organizations to carry out their crimes effectively and safely. In the same way, the determining role that cyberspace plays as a transversal domain to the physical domains of war is addressed, being even named in several countries as the fifth domain that plays a fundamental role in the fight against transnational crimes. Finally, some strategies were formulated that, with institutional synergy, will continue to add efforts in the fight against the scourges of transnational crime in Colombia.

Key words: Cyberspace; Crimes; Domain; Information.

Artículo de Debates
Recibido: 18 de noviembre de 2022 • **Aceptado:** 25 de diciembre de 2022
Contacto: Eduardo Velandia Becerra velandiae@esdeg.edu.co

Introducción

El crecimiento acelerado de la globalización en la última década ha traído grandes retos para las naciones, las estrategias planteadas por los gobiernos a nivel mundial en temas de seguridad y defensa se relacionan con la mutación de las amenazas y, desde su carácter transnacional, también al uso de las tecnologías. El accionar se ha diversificado y atenta contra la soberanía nacional y seguridad.

Desde los inicios del 2000, se ha incrementado los estudios con relación al ciberespacio como un dominio de naturaleza militar. Por este motivo, la conveniencia en potencializar el desarrollo y la búsqueda de capacidades militares en el *ciberespacio* por parte de los actores a nivel mundial. Por consiguiente, el tema ha pasado a ocupar cada vez los espacios más privilegiados en la agenda de gobierno y en relación con los aspectos de la defensa nacional y el diseño de las fuerzas militares (Eissa et al., 2012). El uso del ciberespacio no solo ha sido visto con gran virtud por parte de las instituciones de seguridad de los Estados, sino también posicionado como un elemento que ha surgido como arma invisible al servicio de la criminalidad, trascendiendo fronteras, gobiernos e instituciones en todo el globo terrestre.

Metodología

La presente investigación es de tipo descriptivo, según lo aportado por Hernández, Fernández y Baptista (2014), ya que el objetivo es detallar como son y cómo se manifiestan los fenómenos, situaciones, contextos y eventos. De la misma forma, se busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice.

De igual forma, se aborda un enfoque cualitativo, puesto que se inicia desde la formulación de un problema y se plantea el análisis de este en su desarrollo. Se tiene en cuenta las teorías existentes del tema y, respecto al análisis, se busca formular estrategias partiendo de unos métodos de recolección de datos. El enfoque de la investigación busca describir detalladas de situaciones, eventos, personas, conductas observadas y sus manifestaciones (Escudero & Cortez, 2018).

Caracterización del ciberespacio con los dominios de la guerra

El ciberespacio

Existen diversas definiciones del *Ciberespacio*, sin embargo, se abordan 3 aproximaciones conceptuales; el primero enuncia que es un ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales

(software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios (Comisión Nacional de las Comunicaciones, 2009).

La segunda, no muy alejada de la primera, la define Schmitt (2017) como un ambiente formado por componentes físicos y no físicos para almacenar, modificar y compartir datos usando las redes computacionales.

Y no menos importante, como tercera definición, se entiende de igual forma como un dominio global dentro del ambiente de la información, consistente en redes interdependientes de infraestructura de tecnología de la información, datos contenidos en la internet, las telecomunicaciones, redes, sistemas informáticos, los procesadores y controladores integrados (The National Institute of Standards and Technology, 2012).

Teniendo como base las anteriores definiciones, el ciberespacio se define en este documento como un dominio global dentro del área de la información consistente en un ambiente tanto físico como virtual, este se encuentra compuesto por hardware, software, redes computacionales y sistemas electrónicos. El objetivo es la interacción entre usuarios e implica el almacenamiento, trasmisión, almacenaje y difusión de datos (Cabuya & Mahecha, 2019).

Características del ciberespacio

Dentro del contexto del ciberespacio, se identifican unas características claves que crean una sinergia de factores determinantes en la formación, actualización y uso del mismo, de las cuales se hace referencia a continuación:

Figura 1. Características del ciberespacio

Fuente: Adaptado de Cano (2018) y Choucri (2013).

Como se puede observar, se identifican una serie de características, estas son:

- **Multiplicidad de identidad:** Como factor negativo en muchos casos, pero como mecanismo de gran ayuda en otros, las conexiones e interacciones con las máquinas en los ambientes computacionales ha permitido un nuevo sentido de identidad más *fluido, descentrado* y *múltiple* que se ha construido y transformado mediante el lenguaje informático (Ursua, 2008).
- **Autorregulado**: El ciberespacio, por su misma dimensión, tiende a dificultar su regulación como un todo y más teniendo en cuenta la relatividad de su espacio. Sin embargo, existe normatividad internacional que delimita de forma general con normas éticas para su utilización (Bernal, 2017).
- **Atemporal e instantáneo:** Se caracteriza como una dimensión que no tiene un tiempo determinado, y va más allá del tiempo. De igual forma, se caracteriza por localizar la información que circula en su ambiente de forma instantánea en diferentes lugares al mismo tiempo (Nakasone & Lewis, 2017).
- **Ubicuo:** Que está presente a un mismo tiempo en todas partes (La Real Academia Española, 2020).
- **Permeable:** El ciberespacio tienen algunos materiales físicos que le permite interactuar sin alterar su composición. De la misma manera, esta característica le ofrece la facilidad de no tener fronteras (Alía, 2015).
- **Fluido:** Tiene gran versatilidad, cede con facilidad, fluye constante y ordenadamente sin importar el lugar y la forma del mismo (Merejo, 2008).
- **Participativo:** Como dominio global tiene la facultad de tomar parte activa en innumerables procesos tanto física como en el espacio sideral.

El entorno de la información

Dentro del entorno de la información se determina la composición de un conjunto de individuos, organizaciones y sistemas que recopilan, procesan, difunden o actúan sobre la información. Dado que las *Operaciones en el Ciberespacio* (OC) obedecen a un ciclo lógico, iniciando por la creación, procesamiento, almacenamiento y/o transmisión de información, por ello el ciberespacio estaría contenido en su totalidad en el entorno de la información. Aunado a esto, el entorno de la información sugiere tres divisiones especiales concebidas como las dimensiones física, informativa y cognitiva, e incluye muchos tipos de información que no están en el ciberespacio. Si bien los diferentes tipos de información no contenida en el ciberespacio tiende a disminuir, continúan estando individuos y organizaciones que manejan sus protocolos de información fuera del ciberespacio, en especial cuando los factores de seguridad, durabilidad, costo y alcance son determinantes (United States Department of Defence, 2013).

Relación del ciberespacio con los dominios físicos

Teniendo en cuenta que el ciberespacio forma parte del entorno de la información, como logra hacer una aproximación inicial (United States Department of Defence, 2013), es importante considerar que este depende de los dominios físicos, aéreos, terrestres, marítimos y espaciales -espacio exterior-. Al igual que las operaciones en los dominios físicos, dependen de la infraestructura física creada para aprovechar las características que ocurren naturalmente. Las OC dependen de la infraestructura de tecnología de información integrada en la red, independiente y en plataforma, además de los datos que residen y se transmiten a través de estos componentes, permitiendo la conducción de operaciones militares en un dominio hecho por el hombre.

Las OC usan enlaces y nodos ubicados en los dominios físicos y realizan funciones lógicas para crear efectos en el ciberespacio y luego, según sea necesario, en los dominios físicos. Las acciones en el ciberespacio, a través de efectos en cascada cuidadosamente controlados, pueden permitir la libertad de acción para las actividades en los dominios físicos.

Figura 2. Los cinco dominios de la guerra

Fuente: Cáceres (2020)

Del mismo modo, y teniendo en cuenta a Cáceres (2020), las actividades en los dominios físicos pueden generar efectos en el ciberespacio y afectar el espectro electromagnético o la infraestructura física. La relación entre el espacio y el ciberespacio es única en el sentido de que prácticamente todas las operaciones espaciales dependen del

ciberespacio, y una parte crítica del ancho de banda del ciberespacio solo puede proporcionarse a través de las operaciones espaciales, una opción de conectividad global clave para las operaciones en el ciberespacio.

Por otra parte, el ciberespacio se basa en el *Espectro Electromagnético* (EMS), por ello, el ciberespacio no puede existir sin poder explotar ese dominio espacial que existe de forma natural. Sin este aprovechamiento recíproco, no solo información y tecnologías de la comunicación (TIC) no podrían comunicarse entre ellas, la integración de los circuitos y otros dispositivos microelectrónicos dependen de los electrones para funcionar; los cables de fibra óptica no son nada si no pueden propagar la luz, las redes de TIC también dependen de las innumerables propiedades del EMS por su conectividad esencial a través de radiofrecuencias y microondas (Sheldon, 2011).

En esta misma dirección, los dominios clásicos generan efectos estratégicos en cada uno de los otros sin lugar a dudas, pero el ciberpoder puede generar efectos en todos los espacios de forma absoluta y simultánea, es decir, se podría determinar un carácter de supremacía estratégica en el ámbito de la defensa, ya que las operaciones en el ciberespacio, entendidas como operaciones de información, resultan de interés para los Estados. La importancia de estas operaciones se debe a la capacidad de producir alteraciones y/o modificaciones en el mundo físico, tanto de cualquier dominio como a nivel político (Eissa et al., 2012).

Las relaciones expuestas anteriormente construyen bases sólidas en la importancia y supremacía del quinto dominio de la guerra y su transversalidad con los dominios físicos. Se presenta la siguiente tabla donde se identifican las misiones principales de cada dominio y la misión transversal que cumple el ciberespacio para el apoyo de los demás:

Tabla 1. Relación de misiones de los Dominios de la guerra.

DOMINIOS	MISIONES		
TERRESTRE	Conducir operaciones militares orientadas a defender la soberanía, la independencia y la integridad territorial del Estado al cual pertenece.	Proteger a la población civil, los recursos privados y estatales, neutraliza amenazas internas y externas de los Estados.	Contribuir a generar un ambiente de paz, seguridad y desarrollo, que garantiza el orden constitucional de las naciones.
NAVAL	Contribuir a la defensa de la nación con un poder naval flexible en los espacios marítimo, fluvial y terrestre bajo su responsabilidad.	Protección de la soberanía y seguridad de la nación. Cumplir la función constitucional y participar en el desarrollo del poder marítimo y la protección de los intereses de los colombianos.	La ARC contribuye día a día a la recuperación y consolidación de la paz y la seguridad de los colombianos, garantizando el uso legítimo de los espacios marítimos y fluviales del país, con base en la proyección de una capacidad disuasiva y operacional.

Continúa tabla...

DOMINIOS	MISIONES		
AÉREO	Fuerza ejerce y mantiene el dominio del espacio aéreo, conduce operaciones aéreas para la defensa de la soberanía, la independencia, la integridad del territorio nacional, el orden constitucional y el logro de los fines del Estado.	El espacio aéreo es la esencia de la Fuerza Aérea, es su razón de ser, no sólo como Fuerza de defensa activa y pasiva al servicio de la nación, sino como Fuerza decisiva para un futuro en paz y armonía para el pueblo colombiano.	La Fuerza Aérea Colombiana tiene la tarea de conducir no sólo operaciones aéreas con sus aeronaves, sino que es responsable de la conducción doctrinal de toda la aviación colombiana.
ELECTROMAGNÉTICO		**CIBERESPACIAL**	
Prevenir, contrarrestar y negar el uso del espectro electromagnético por parte del enemigo y asegurar el empleo del mismo por parte de las Fuerzas amigas. Se debe neutralizar el ataque del adversario a través de la ejecución conjunta y coordinada de acciones de guerra electrónica, que permitan desarrollar tareas de recolección y análisis de información de la amenaza, detección oportuna y empleo coordinado y sincronizado de medios cinéticos y no cinéticos.		La misión principal es neutralización de ataques en el ciberespacio a través de operaciones militares. Para la neutralización de estos ataques, la Fuerza Pública debe proteger la información y los sistemas mediante la prevención, detección, reacción y recuperación de ataques, intrusiones, interrupciones u otras acciones hostiles deliberadas, recopilar información sobre sistemas de información de potenciales adversarios. También debe tomar medidas y acciones para interrumpir, negar, degradar o destruir la información manejada por los sistemas de información y comunicaciones del posible adversario. De esta manera, la Fuerza Pública logra mediante el ciberespacio proveer un apoyo transversal como capacidad al cumplimiento de las misiones de los demás dominios.	

Fuente: Ministerio de Defensa Nacional (2016) p. 17,18,19,20 y 51.

Modelo de capas del ciberespacio.

Para facilitar la planificación y ejecución de las OC, se describe al ciberespacio en términos de tres capas interrelacionadas: *Red Física, Red Lógica y Ciber-Persona* (Figura 3). Cada capa representa un enfoque diferente desde el que se puede planificar, realizar y evaluar las OC (United States Department of Defence, 2013).

Figura 3. *Capas del Ciberespacio*

Fuente: Adaptado de United States Department of Defence (2013)

- **Capa de red física**: Consiste en los dispositivos de tecnologías de la información y la infraestructura en los dominios físicos que proporcionan almacenamiento, transporte y procesamiento de información dentro del ciberespacio, incluyendo los repositorios de datos y las conexiones que transfieren datos entre los componentes de la red. Los componentes físicos de la red incluyen el hardware y la infraestructura -por ejemplo, dispositivos informáticos, dispositivos de almacenamiento, dispositivos de red y enlaces cableados e inalámbricos-.

  Los componentes de la capa de red física requieren medidas de seguridad física para protegerlos de daños físicos o acceso físico no autorizado, que pueden aprovecharse para obtener acceso lógico. La capa de red física es el primer punto de referencia que utilizan las OC para determinar la ubicación geográfica y el marco legal apropiado.

  Si bien los límites geopolíticos pueden cruzarse fácil y rápidamente en el ciberespacio, todavía hay problemas de soberanía relacionados con los dominios físicos. Cada componente físico del ciberespacio es propiedad de una entidad pública o privada, que puede controlar o restringir el acceso a sus componentes.
- **Capa de red lógica:** Consiste en aquellos elementos de la red relacionados entre sí de una manera abstraída de la red física, en función de la programación lógica (código) que controla los componentes de la red. Es decir, las relaciones no están necesariamente vinculadas a un enlace o nodo físico específico, pero pueden ser abordadas de forma lógica e intercambiar o procesar datos). Los enlaces y nodos individuales están representados en la capa lógica, pero también lo están los diversos elementos distribuidos del ciberespacio, incluidos los datos, las aplicaciones y los procesos de red que no están vinculados a un solo nodo.
- **Capa ciber-persona:** Es una vista del ciberespacio creado al abstraer datos de la capa de red lógica utilizando las reglas que se aplican en esta capa para desarrollar descripciones de representaciones digitales de una identidad de actor o entidad en el ciberespacio (ciber-persona). La capa de ciber-persona consiste en cuentas de usuario de red o de TI, ya sean humanas o automatizadas, y sus relaciones entre sí.

  Las ciber-personas pueden relacionarse directamente con una persona o entidad real, incorporando algunos datos personales u organizativos (por ejemplo, correo electrónico y direcciones IP, páginas web, números de teléfono, inicios de sesión en foros web o contraseñas de cuentas financieras). Una persona puede crear y mantener múltiples personas cibernéticas mediante el uso de múltiples identificadores en el ciberespacio, como direcciones de correo electrónico personales y de trabajo separadas, y diferentes identidades en diferentes foros web, salas de chat y sitios de redes sociales. A la inversa, una sola

ciber-persona puede tener múltiples usuarios (ejemplo, adversarios que usan el mismo alias de control de software malicioso (malware), varios adversarios que usan una sola cuenta bancaria o todos los miembros de la misma organización que usan la misma dirección de correo electrónico) (United States Department of Defence, 2013).

El uso de ciber-personas puede dificultar la atribución de responsabilidades por acciones en el ciberespacio. Debido a que las personas cibernéticas pueden ser complejas, con elementos en muchas ubicaciones virtuales que no están vinculados a una sola ubicación o forma física, su identificación requiere una recopilación y un análisis de inteligencia significativos para brindar una visión y una conciencia suficientes de las situaciones para permitir la focalización efectiva o para crear el efecto deseado. Al igual que la capa de red lógica, los cambios complejos en las ciber-personas pueden ocurrir muy rápidamente en comparación con cambios similares en la capa de red física, lo que complica las acciones contra estos objetivos sin un seguimiento detallado de los cambios (Saz, 2016).

Ciberespacio basado en la locación y propiedad

El ciberespacio es complejo y, generalmente, no es observable. Por lo tanto, el personal que planifica ejecuta y evalúa las OC, pueden describir el ciberespacio según la ubicación o la propiedad, de manera que ayude a una rápida comprensión de las operaciones planificadas, como se observa en la Figura 2.

El término ***Ciberespacio azul*** denota áreas en el ciberespacio protegidas por Colombia, sus aliados en la misión, Infraestructuras Críticas Cibernéticas Nacionales, intereses nacionales y otras áreas a las que el Gobierno Nacional ordene proteger.

El término ***Ciberespacio Rojo*** se refiere a aquellas partes del ciberespacio propiedad o controladas por un adversario o enemigo. En este caso, *controlado* significa más que simplemente *tener presencia,* ya que las amenazas pueden tener acceso clandestino a elementos del ciberespacio mundial donde su presencia no se detecta y sin un impacto aparente en el funcionamiento del sistema. Igualmente, *controlado* significa la capacidad de dirigir las operaciones de un enlace o nodo del ciberespacio, con exclusión de otros.

Todo ciberespacio que no cumpla con la descripción de *azul* o *rojo* se conoce como ***Ciberespacio Gris***.

Figura 4. Locación y propiedad del ciberespacio

Fuente: Elaboración propia. Adaptado de (Eissa et al., 2012).

Conectividad y acceso en el ciberespacio

El ciberespacio se compone de innumerables y diferentes elementos superpuestos que incluyen redes, nodos, enlaces, aplicaciones interrelacionadas, datos de usuario y datos del sistema. Aunque el ciberespacio continúa estando cada vez más interconectado, algunos elementos se aíslan o subdividen intencionalmente en enclaves mediante controles de acceso, cifrado, protocolos únicos o separación física. Con la excepción del aislamiento físico real, ninguno de estos enfoques elimina la conectividad física subyacente; en cambio, limitan el acceso a la red lógica.

El acceso, ya sea autorizado o no autorizado, se puede obtener a través de una variedad de medios. Si bien las OC requiere conectividad, accesos oportunos y efectivos, es posible que el gobierno nacional no posea, controle ni tenga acceso a la infraestructura necesaria para respaldar las operaciones militares (United States Department of Defence, 2013).

Sobre la misma línea documental, el acceso significa un nivel suficiente de exposición, conectividad o entrada a un dispositivo, sistema o red para permitir operaciones adicionales dentro del marco legal correspondiente. Si bien algunos accesos se pueden crear de forma remota con o sin el permiso del propietario de la red, el acceso a redes cerradas y otros sistemas que están virtualmente aislados puede requerir la proximidad física o procesos más complejos. Además, el acceso a áreas operacionalmente útiles del ciberespacio, incluidos los objetivos dentro de ellos, se ve afectado por limitaciones

legales, políticas u operativas. Por todas estas razones, el acceso no está garantizado (Medina-Ochoa, 2019).)

Declaración de divulgación

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

Autor

Eduardo Velandia Becerra. Magíster Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra, Colombia. Diplomado Oficial de Estado, Escuela Superior de Guerra, Colombia. Diplomado de Seguridad y Defensa Nacional, Escuela Superior de Guerra, Colombia. Diplomado en Prevención de Riesgos, Escuela de Inteligencia y Contrainteligencia, Colombia. Diplomado Internacional de Crimen Trasnacional y Redes de Terrorismo Internacional como Factores de Amenazas Híbridas, Embajada de Americana. Especialista en Administración de Recursos para la Defensa Nacional, Centro de Educación Militar, Colombia. Instructor Training Course, Instituto de Cooperación para la Seguridad Hemisférica, Estados Unidos. Instructor Training Small Groups, Instituto de Cooperación para la Seguridad Hemisférica, Estados Unidos. Profesional en Ciencias Militares, Escuela Militar de Cadetes General, Colombia.

ORCID: https://orcid.org/0009-0006-8695-5765
Contacto: velandiae@esdeg.edu.co

Referencias

Alía Plana, J. (2015). Reglas de enfrentamiento y gobierno del Campo de Agramante. *Revista del Instituto Español De Estudios Estratégicos,* (5), 201–232.

Bernal, Á. É. (2017). *El ciberespacio. Un mundo sin ley*. http://ciberderecho.com/El_ciberespacio_un_mundo_sin_ley.pdf

Cabuya D., & Mahecha A. (2019). *Lineamientos Estratégicos de Ciberdefensa para el Comando General de las Fuerzas Militares de Colombia*. [Reservado]. Comando Conjunto Cibernético.

Cáceres García, J. A. (2019) Ciberespacio, nuevo medio de amenaza a la seguridad ciudadana. Ciberdelitos: tráfico de drogas y violencia. ¿Ficción o realidad?. *Revista de las Fuerzas Armadas*, 248, 32–38.

Cano, J. (2018). *Memorias Congreso Internacional Ciberseguridad Escuela Superior de Guerra*. Escuela Superior de Guerra.

Choucri, N. (2013). Cyberpolitics in international relations. *Choice Reviews Online*, 50(12), 50-6993-50–6993. https://doi.org/10.5860/choice.50-6993

Comisión Nacional de las Comunicaciones. (2009). *Resolución 2258 de 2009*. https://itcomunicaciones.net/Resolucion 2258.pdf

Eissa, S., Gastaldi, S., Poczynok, I., & Zacarías, M. (2012). *El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino*. VI Congreso de Relaciones Internacionales, 1–19. https://core.ac.uk/download/pdf/296371994.pdf

Escudero, C., & Cortez, L. (2018). Técnicas y métodos cualitativos para la investigación científica. In Redes 2017.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de Investigación. Metodología de la investigación*. McGraw-Hill. http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdfv

La Real Academia Española. (2020). *Ubicuo*. La Real Academia Española (RAE). https://dle.rae.es/ubicuo

Medina-Ochoa, G. E. (Ed.). (2019). *La Seguridad en el Ciberespacio: Un desafío para Colombia*. Sello Editorial ESDEG. https://doi.org/10.25062/9789585216549

Merejo, A. (2008). La complejidad en el ciberespacio. *Revista de Filosofía*, IV (24).

Ministerio de Defensa Nacional. (2016). *Visión de Futuro de las Fuerzas Armadas*. Imprenta Nacional de Colombia.

Nakasone, P. M., & Lewis, C. (2017). Cyberspace in Multi-Domain Battle. *The Cyber Defense Review*, 2 (1), 15–26. http://www.jstor.org/stable/26267397

Saz, B. M. (2016). *CyberCamp.es Mando Conjunto de Ciberdefensa*. https://www.incibe.es/sites/default/files/contenidos/material/cybercamp2016-operaciones_militares_en_el_ciberespacio-mccd_manuel_saz.pdf

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge: Cambridge University Press. doi:10.1017/9781316822524

Sheldon, J. B. (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly*, 95–112. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA544498

The National Institute of Standards and Technology. (2012). *Cyberspace - Glossary | CSRC*. https://csrc.nist.gov/glossary/term/cyberspace

United States Department of Defence. (2013). *Cyberspace Operations*. Joint Publication 3-12.

Ursua, N. (2008). *La(s) identidad(es) en el ciberespacio. Una reflexión sobre la construcción de las identidades en la red ("online Identity")*. https://core.ac.uk/download/pdf/13303445.pdf

Coyuntura

Defiances

Esta página queda intencionalmente en blanco

Revista Ciberespacio, Tecnología e Innovación
Volumen 1, número 2, julio-diciembre 2022 (pp. 181-186)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

La regulación del ciberespacio como principal ecosistema de la cuarta revolución industrial

The regulation of cyberspace as the main ecosystem of the fourth revolution industrial

DOI: https://doi.org/10.25062/2955-0270.4776

Julián Alberto González Moreno
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

Este momento disruptivo presenta un reto complejo para las naciones, ya que las acciones para construir la regulación de esta incursión tecnológica no van a la velocidad de su avance. Este escrito presenta un análisis desde la óptica de tres autores en las que se exponen las percepciones sobre el rol de un estado para generar las acciones necesarias que respondan a estos desafíos. Finalmente, concluye con una propuesta analógica, basada en las buenas prácticas de regulación del espectro electromagnético, implementada por la Unión Internacional de Telecomunicaciones (UIT).

Palabras Clave: ciberespacio, dominio, tecnología

Abstract

This disruptive moment presents a complex challenge for nations since the actions to build the regulation of this technological incursion are not keeping pace with its advance. This paper presents an analysis from the perspective of three authors in which the perceptions of the role of a state in generating the necessary actions that respond to these challenges are presented. Finally, it concludes with an analogue proposal, based on good practices for regulating the electromagnetic spectrum, implemented by the International Telecommunications Union (ITU).

Key words: cyberspace, domain, technology

Artículo de Coyuntura
Recibido: 8 de noviembre de 2022 • **Aceptado:** 1 de diciembre de 2022
Contacto: Julián Alberto González Moreno julian.gonzalezm@esdeg.edu.co

Ciberespacio como principal ecosistema de la cuarta revolución industrial

La humanidad ha atravesado por 4 revoluciones industriales en los últimos tres siglos, las cuales han cambiado de manera definitiva su curso. Es de resaltar, que el intervalo entre cada revolución ha sido más corto con respecto a la anterior (Martínez, 2016). Justo ahora, se desarrolla la cuarta revolución industrial en la que el mundo tiene una creciente participación en el entorno digital y una dependencia y uso creciente de las tecnologías que se involucran en el ciberespacio (Consejo Nacional de Política Económica y Social, 2019).

Primero que todo, teniendo en cuenta que la cuarta revolución está basada en el uso del internet para conectar el mundo (Martínez, 2016), es claro que la democratización de la información en el ciberespacio es un hecho ineludible e inevitable para la humanidad. El ciberespacio, según la declaración de John Perry Barlow (1996) no se encuentra enmarcado ni contenido en fronteras, gobiernos o corporaciones específicas. No hay medidas efectivas para evitar que los controles rigurosos de algunos estados eviten restringir con políticas tradicionales la globalización creciente de la información en el ciberespacio (Barlow, 1996). A pesar de que su perspectiva sobre el ciberespacio se dio en un momento en el que el internet estaba apenas en su expansión temprana, hoy en día, su discurso se ajusta perfectamente a la realidad. Ahora más que nunca, el ciberespacio se ha desarrollado y ha evolucionado de manera inesperada, trascendiendo del actuar y la influencia de actores como los gobiernos o la industria tradicional (Barlow, 1996). En su discurso es notorio su afán de libertad y emancipación. No obstante, hace más de 20 años no se tenía un estimado de la dimensión de los posibles impactos negativos y amenazas sobre una sociedad que no ejerce control sobre el ciberespacio.

Precisamente, Post & Johnson (1997) hablan sobre romper las fronteras territoriales en el ciberespacio, es decir, que este no debe ser sometido a la jurisdicción de un estado en las mismas condiciones de sus leyes territoriales. El ciberespacio es un dominio y entorno que trasciende estas fronteras a nivel mundial (Johnson & Post, 1997) y esto significa que solapa culturas, ideologías, marcos legales y regulatorios específicos de cada nación. Adicionalmente, los autores enfatizan que la información no tiene una ubicación geográfica definida, por lo que simplemente se reduce a la interacción de una pantalla y una contraseña (Post & Johnson, 1997).

En consecuencia, esta realidad presenta un reto complejo para que un gobierno pretenda ejercer soberanía sobre la influencia, los recursos y la información del ciberespacio, tal como lo hace en el entorno físico de su territorio para aplicar su poder, control, gestión y dominio. De todas maneras, esto no significa que no sea posible o viable; es claro que todo estado debe velar por sus intereses y los de su nación.

El punto álgido está en cómo ejercer y emitir leyes y regulaciones que persistan y se apliquen de manera lógica y acorde a las tendencias tecnológicas y que, además, no

vayan en contraposición o supriman el desarrollo y el derecho al acceso a la información, tan imprescindible para la sociedad actual. Es precisamente el arte y ciencia que permitan desarrollar la legislación adecuada, pero rompiendo los paradigmas de las leyes definidas para ámbitos geográficos (Post & Johnson, 1997).

Teniendo en cuenta lo anterior, se podría generar un contraste en el que se visualicen los efectos de un mayor control por parte de los gobiernos sobre el ciberespacio. Por una parte, un estado podría generar políticas, leyes y regulaciones con el fin de controlar el contenido de influencia no deseado, entendiendo que este podría afectar o desestabilizar su plan de gobierno o su ideología. Sin embargo, este control puede desencadenar la coacción de derechos de libertad de expresión, haciendo que el estado tome un papel opresor o dictador. Por otra parte, un gobierno puede tomar las medidas de control necesarias y amplias para mitigar y prevenir el cibercrimen en su territorio, pero un control exagerado hará que su población se aísle del ambiente de la información que requerirá para su desarrollo en diferentes ámbitos.

Finalmente, se podría limitar el tráfico de información mediante la intervención física de los canales terrestres de comunicaciones para condicionar el acceso a determinadas plataformas o portales, los cuales se consideren inconvenientes de acuerdo con políticas o planes de gobierno establecidos. No obstante, debe tenerse en cuenta que hoy en día las tecnologías de internet satelital, tanto en órbita geoestacionaria como órbitas bajas, pueden brindar cobertura a estaciones terrestres sin que haya posibilidad o mecanismos de intervención o impedimento por parte del estado.

Entonces, en este punto se abre la discusión sobre cuál sería la manera o metodología óptima para poder afrontar la realidad del control que demanda el ciberespacio en la época actual, teniendo en cuenta el impacto en todos los ámbitos la sociedad ya considerada como digital. Es aquí en donde el enfoque de Lessig nos brinda un marco de entendimiento y una posible solución para abordar el problema de la regulación que debe imponerse en el ciberespacio.

De acuerdo con los autores citados, ya es claro que se requieren garantías de libertad en el acceso a la información valiosa en internet para el desarrollo de una nación. También es evidente que, si bien el ciberespacio no tiene fronteras tangibles, requiere de un control adaptado a su contexto y realidad. La pregunta es cómo hacerlo de manera efectiva para que no afecte el gobierno, la industria y el mercado.

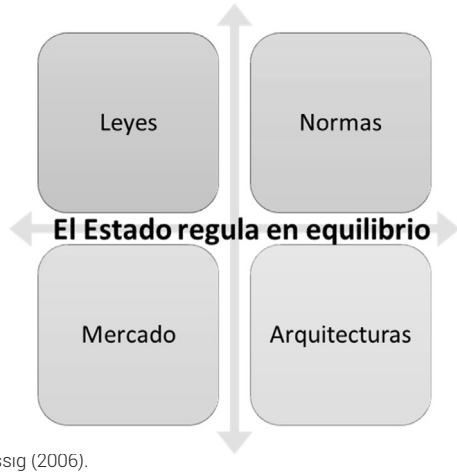
Lessig hace un análisis holístico en el que concluye que el esfuerzo de la regulación no debe ser impulsado por un sector en específico (Lessig, 2006), pues si fuera de esa manera, las condiciones propuestas se inclinarían a intereses particulares que, en últimas, llegarían a extremos negativos ya acontecidos y comprobados en la historia (Lessig, 2006). Ejemplos de lo anterior apuntan al monopolio, ya sea de estados o compañías que

pretendan someter, bajo sus propios intereses, las condiciones del ciberespacio. Por lo tanto, después de un análisis exhaustivo, Lessig indica que la mejor manera de establecer un control sano sobre el ciberespacio se logra mediante la articulación de cuatro componentes denominados: leyes, normas, mercado y arquitecturas (Lessig, 2006).

Bajo el análisis mencionado, Lessig propone la regulación del estado de manera indirecta, modulando cualquiera de los otros componentes, ya sea el mercado, las normas o la arquitectura, para lograr un efecto deseado que no condicione la libertad de manera explícita. En este sentido y de forma responsable, se pueden generar interacciones que equilibren el control que se requiere sin llegar a extremos y sin caer víctimas de corrientes políticas de turno que pueden hacer más daño que la misma falta de regulación o control.

Existen diferentes ejemplos de este modelo, en otros ámbitos, que ya han sido implementados con éxito. Uno de ellos, y tal vez el más cercano por su afinidad tecnológica, es la regulación del uso del espectro electromagnético a nivel global, el cual es armonizado y orientado por parte de la Unión Internacional de Telecomunicaciones (UIT). De hecho, la UIT es la entidad adscrita de las Naciones Unidas para las tecnologías de la información y la comunicación (UIT, 2023). Esta organización atribuye el espectro de frecuencias radioeléctricas y las órbitas satelitales, elabora normas técnicas para garantizar la interconexión armoniosa de redes y tecnologías y propende por el mejoramiento de acceso a las TIC para las comunidades a nivel global (UIT, 2023).

Figura 1. Equilibrio componentes con intervención del Estado



Fuente: Adaptado de Lessig (2006).

La UIT se compone de 193 estados miembros, así como 900 empresas, universidades y organizaciones internacionales y regionales, de tal manera que, conforma un escenario perfecto para las interacciones entre el sector público y privado a nivel global

(UIT, 2023). El territorio mundial está dividido en tres regiones, las cuales también tienen organizaciones y comisiones que definen las posiciones y regulaciones para el uso del espectro. Constantemente, estas organizaciones establecen mesas de trabajo y reuniones para tomar decisiones de regulación en las que se incluyen los gobiernos, pero también el sector de la industria y el mercado, pues son ellos quienes impulsan el desarrollo tecnológico. Este es un ejemplo exitoso de la integración que propone Lessig y que eventualmente podría ser una hoja de ruta para el futuro de la regulación en el ciberespacio.

Conclusión

En conclusión, el impacto que trae la cuarta revolución industrial está impulsando la disrupción que transforma todos los sectores de la economía y el desarrollo. Para esto se requiere de un entorno digital seguro y confiable que esté acorde con el aumento y dinamismo de la sociedad, los gobiernos y las corporaciones que traen progreso al mundo (CONPES, 2019, p. 10). Como se mencionó al inicio, de seguro, la regulación del ciberespacio vendrá más lento que los avances tecnológicos; sin embargo, se debe lograr un equilibrio que garantice la libertad, el desarrollo, la integridad, la legitimidad y el bienestar de la población en general, para que los diferentes actores logren una armonización que establezca normas generales y aplicables de forma transnacional.

De igual manera, es importante buscar las estrategias para lograr consensos, aprovechando las organizaciones y acuerdos globales existentes, que busquen armonizar la regulación del uso del ciberespacio. Para este propósito, se deben intensificar los esfuerzos de cooperación y trabajo de relaciones internacionales, con el fin de generar propuestas comunes, fuera de intereses apegados a los ámbitos del poder específico de un sector, potencia o gobierno.

Declaración de divulgación

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

Autor

Julián Alberto González Moreno. Mayor del Ejército Nacional de Colombia. MSc. en Ingeniería de la Ciberseguridad, Tallinn University of Technology, Estonia, Máster en Transformación Digital y Desarrollo de Negocio, Universitat de Barcelona, España y Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia.

ORCID: https://orcid.org/0000-0002-6463-6708
Contacto: julian.gonzalezm@esdeg.edu.co

Referencias

Barlow, J. P. (8 de Feb de 1996). *Una Declaración de independencia del ciberespacio*. Obtenido de Electronic Frontier Foundation: https://www.eff.org/cyberspace-independence

Barlow, J. P. (1996). *Declaración de independencia del ciberespacio*. http://homes. eff. org/% 7Ebarlow/Declaration-Final. html.

Consejo Nacional de Política Económica y Social. (11 de Octubre de 2019. *Departamento Nacional de Planeación de la República de Colombia*. Obtenido de Política Nacional de Confianza y Seguridad Digital. https://www.dnp.gov.co/CONPES/Documents/2019-10-11%20Documento%20CONPES%20Pol%C3%ADtica%20de%20Confianza%20y%20Se guridad%20Digital.pdf

Johnson, D. R., & Post, D. G. (1 de febrero de 1997). *Ley y fronteras - El nacimiento de la ley en el ciberespacio.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535

Lessig, L. (2006). *Código, versión 2.0.* Park Avenue South, New York, NY 10016–8810: Basic Books.

Martínez, A. R. (27 de Feb de 2016). *Las cuatro revoluciones industriales y el progreso*. Obtenido de Confidencial. https://confidencial.com.ni/las-cuatro-revoluciones-industriales-y-el- progreso/

UIT. (05 de febrero de 2023). *Sobre la Unión Internacional de Telecomunicaciones (UIT).* https://www.itu.int/es/about/Pages/default.aspx

Perspectivas

Perspectives

Esta página queda intencionalmente en blanco

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 1, número 2, julio-diciembre 2022 (pp. 189-192)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Entrevista a Steven Jones-Chaljub. El ciberespacio humano: retos y perspectivas

Interview with Steven Jones-Chaljub. Human cyberspace: challenges and perspectives

DOI: https://doi.org/10.25062/2955-0270.4781

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

Biografía

Magister en Seguridad Internacional, University of Warwick, Reino Unido. Magister en Estudios Estratégicos, Nanyang Technological University, Singapur. Profesional en Negocios Internacionales, Universidad EAFIT. Se ha desempeñado como consultor en estudios internacionales para diferentes tanques de pensamiento. Fue docente e investigador en la Escuela Superior de Guerra "General Rafael Reyes Prieto", y asesor de Fuerzas Militares de Colombia y el Ministerio de Defensa Nacional.

Entrevista
Recibido: 14 de octubre de 2022 • **Aceptado:** 5 diciembre de 2022
Contacto: Fabián Cristancho Rodríguez gacademicomaeci@esdeg.edu.co

Entrevista a Steven Jones-Chaljub. El ciberespacio humano: retos y perspectivas

Con ocasión a la creación de su libro *Contextualización del ciberespacio humano* cuéntenos ¿Cuál fue la motivación de adentrarse en el estudio del cibersespacio desde la perespectiva humana?

Realmente el ciberespacio es maravilloso porque es el único entorno creado por la humanidad, digamos que nosotros en la existencia de los dominios de la guerra hablamos del espacio, el aire, la tierra, el mar, los ríos y demás, y los tratamos como entornos en los que interactuamos y proyectamos poder, sin embargo, por primera vez en la historia hemos creado algo nuevo, algo donde nosotros somos, con un poco de egocentrismo humano, los creadores, amos y señores de este entorno. Bajo esta perspectiva, este entorno intangible, nos posibilita a visibilizar inquietudes que superan lo técnico, más allá del hardware o software tenemos inquietudes que incluso desde la sociología se han dado y es allí en donde la investigación encuentra su inicio.

Parte de los retos del ciberespacio ha sido repensar la manera en la que convivimos con multiples cosas, no solo en la cotidianidad sino por ejemplo, en la manera de ejercer ciudadania, de interactuar con el Estado, e incluso la manera de configurar las relaciones interpersonales, puesto que existe una marcada tendencia a desconfiar de los dispositivos o los programas que están configurados desde la inteligencia artificial por el temor de un "reemplazo". Sobre esta base ¿Cómo eliminar la desconfianza con la inteligencia artifical como tecnología disruptiva?

Yo creo que satanizar una herramienta es un despropósito. La inteligencia artificial es una herramienta más que no estamos entendiendo realmente. En la actualidad, podriamos equiparar a una carrera de desarrollo nuclear en el pasado con lo que hoy en día es la carrera del desarrollo de las inteligencias artificales que genuinamente no sabemos para qué la queremos. Por supuesto, se conoce que la IA nos facilita un sinfín de tareas, permitiendo el tratamiento de información, automatización, entre otras, pero la historia de la humanidad ha desmostrado que las herramientas terminan pervirtiendose o saliéndose de control, lo mismo pasó con el TNT o con la energia nuclear.

Esta preocupación ya existe, si observamos los debates de la Organización de las Naciones Unidades, hay una discusión muy seria respecto a los sistemas de armas autónomas letales, en las que vemos materializadas diversas ideas cinematográficas que solo se pensaba podían ocurrir en la ciencia ficción. Por tal motivo, se ha

propendido por la restricción en cierta media frente a la creación de estas herramientas, ubicando como límite la antropomorfización, no debería tener un cuerpo humano a un arma letal.

Finalmente, para mí el problema real es el nivel de autonomía que se le da a la inteligencia artíficial, partiendo del cuestionamiento si el desarrollo por el desarrollo merece la pena que se haga de forma libre y sin control, o deben empezarse a ubicar reglas y límites claros. Con todo, hay que hacer un alto y analizar a dónde se va a llegar con el desarrollo de las herramientas autonomas que han sido y siguen siendo creadas por humanos.

¿Cómo se identifica el poder y las relaciones interpersonales en el ciberespacio?

Si el ciberespacio es una proyección de la voluntad de las personas, se entiende entonces que existen las *ciberpersonas*, siendo este un concepto que aun no se desarrolla en teoría y mucho menos en la normatividad, de hecho ahora mismo estoy trabajando en ello, con el ánimo de identificar ¿quién es el individuo en el ciberespacio? Más aun cuando las acciones en este entorno tienen implicaciones en el mundo real. Sin duda, el debate es obtuso, incluso un poco extraño.

Si yo convivo en una comunidad digital ¿qué derechos u obligaciones tengo en la misma? Y así mismo ¿cómo se ejerce la soberanía allí? Tales preguntas quizá podrían visibilizarse en quiénes son los dueños del servicio y así mismo cómo se aceptan los terminos y condiciones por ejemplo, en Facebook o Twitter. El desarrollo del poder es complejo y no está intimamente relacionado con los Estados pues hay interacciones que son reguladas por administradores privados. Con ello, el poder que se gesta de las interacciones extraciberespaciales y las interciberespaciales no tienen correspondiencia con el concepto de soberanía que manejamos.

Por último ¿Cómo mejorar la interacción humana con el ciberespacio? ¿cuál sería entonces la respuesta para que las personas puedan interactuar bien con el ciberespacio y al final, por ejemplo, sus datos no siempre estén a merced del otro?

Yo creo que en este momento vivimos en un mundo hiper conectado, hay muy pocas personas que no hacen parte del ciberespacio, la gran mayoría de personas están conectadas desde lo más básico en un celular, hasta en las empresas con equipos sofisticados. Para mí entonces el principal consejo es entender la responsabilidad como usuario, es que mira, tú no le entregas las llaves de tu casa a un desconocido, o tú no vas por la calle diciendo que vas a regalar un millón de pesos. Hoy por hoy los

datos son eso, los datos son las llaves de tu casa o son dinero, y no solamente en el punto de vista de tu cuenta bancaria, sino del metadata y las empresas se lucran de tu información personal sin que te des cuenta.

Es claro que hay errores que la inmediatez nos hace cometer y que son fatídicos. Por ejemplo, compartir información privada, o de las empresas e instituciones vía WhatsApp, olvidando que la información se puede reenviar o se le puede dar un mal uso. Yo creo que lo importante es ser consciente de las herramientas y los permisos que otorgas. Adicional a la formación en los colegios, enseñándoles cómo se debe interactuar de manera correcta, impidiendo que se destruya la vida y la intimidad personal con un mal comentarios o información falsa.

Autora de la entrevista

Fabián Cristancho Rodríguez. Magister en Seguridad y Defensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Profesional en Relaciones Internacionales de la Universidad Nuestra Señora del Rosario. Con formación para el análisis de procesos históricos, geopolíticos, socioeconómicos y culturales de la sociedad nacional e internacional.

ORCID: https://orcid.org/0009-0008-0057-5732
Contacto: gacademicomaeci@esdeg.edu.co

Enfoques

Insights

Esta página queda intencionalmente en blanco

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 1, número 2, julio-diciembre 2022 (pp. 195-197)
Bogotá, D.C, Colombia

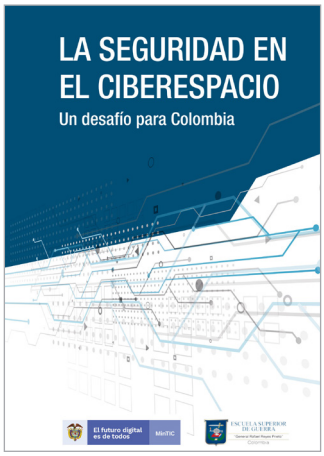
EDITORIAL **ESDEG**

Reseña de libro. La ciberseguridad, sus impactos y desafíos

Book review. Cybersecurity, its impacts and challenges

DOI: https://doi.org/10.25062/2955-0270.4801

Viviana Pilar Fuquen Flautero
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia



Autores del libro: **René Leiva Villagra, Hernán Díaz Mardones, René Leiva Villagra, Mario Arteaga Velásquez, Carl Marowski Pilowsky y Mario Polloni Contardo**
Editorial: Centro de Estudios Estratégicos CEEAG
Año: 2018
ISBN impreso: 978-956-7734-09-2
Páginas: 168

El libro *La ciberseguridad, sus impactos y desafíos* es una compilación de siete capítulos de diferentes autores que abordan la transformación de la guerra en el ciberespacio, un ambiente complejo que cada vez despierta más el interés de expertos y académicos en el ámbito militar, también resulta ser un nuevo eje de investigación en Centro de Estudios Estratégicos de Chile, una institución que es referente en el ámbito estratégico defensa.

En el primer capítulo titulado *Aparece la ciberguerra* se abordan las bases de la ciberguerra. En este se abordan los aspectos conceptuales del ciberespacio y cómo se proyectan desde una visión estratégica moderna, dónde el usuario, la infraestructura, los protocolos y los sistemas operativos interactúan a la par del desarrollo tecnológico. Como ideas principales, se establece la transformación de la guerra, lo cual implica

transformar el pensamiento tradicional y contemplar medios y métodos para desarrollar un conflicto desde el ámbito ciberespacial.

En el segundo capítulo, *Infraestructura crítica vulnerable a la ciberguerra*, afirma que existen unas ventajas y unas oportunidades en el ámbito de la información y las telecomunicaciones, pero en el ciberespacio donde todo interactúa como una red de interconexión que requiere, necesariamente, de infraestructura crítica entendida como las capacidades técnicas y organizacionales relacionadas con activos estratégicos y que son importantes para la sociedad.

Entre los aspectos importantes a señalar en este apartado, se encuentra que la ciberguerra, en los últimos años, ha convertido la infraestructura crítica en un objetivo estratégico para las naciones que pueden desarrollar hostilidades en el ciberespacio, por tal motivo se requiere el desarrollo e instalaciones, redes, servicios y equipos físicos de alta tecnología que se encuentran articuladas en una estrategia de seguridad nacional desde el ciberespacio, esto con el objetivo de contener las amenazas y reducir los riesgos a infraestructuras importantes como la energética, los servicios financieros, la seguridad pública, el transporte y la defensa.

En tercer capítulo, *La lógica de la ciberguerra y su relación compleja con la disuasión*, en este escrito se analiza de manera crítica lo que significa la complejidad de las amenazas y el riesgo que se generan a través del ciberespacio. Conceptos como ciberdefensa y ciberseguridad son el motivo de análisis en este apartado, reconociendo que son dos ámbitos que se complementan para mantener la confiabilidad, integridad y disponibilidad de la información a manera de una *tríada*. Adicionalmente, se resaltan las múltiples amenazas que existen en la red, destacando que también existen unos riesgos relacionados con la infraestructura y las capacidades tecnológicas de los Estados. Como conclusión, se afirma que el ciberespacio se está consolidando como un factor estratégico que requiere que el campo de la defensa oriente una estrategia de seguridad y desarrolle medidas de prevención, disuasión, protección y reacción de la ciberdefensa.

El cuarto capítulo, *El desafío del combate por el mando y control,* analiza dos conceptos importantes en el desarrollo de las hostilidades: El mando y control. Es importante que exista un desarrollo doctrinal debido a que existe una creciente necesidad de contener amenazas y riesgos generados por las diferentes tipologías de guerra entre las cuales se destaca la guerra electrónica y la guerra de la información. Es por esto que en el marco del desarrollo de las operaciones de combate debe existir el mando y el control, entendiendo que existe un quinto dominio de la guerra basado en la información y en donde se deben establecer estrategias defensivas y ofensivas.

El quinto capítulo, *Efectos de los riesgos y amenazas de la ciberguerra en la infraestructura crítica*, se realiza un importante análisis sobre los efectos de los riesgos y amenazas de la ciberguerra en la infraestructura crítica. Complementando los análisis

anteriores, en este apartado se resalta el efecto que puede causar la guerra en el ciberespacio a la infraestructura crítica, afirmando que existe un alto nivel de riesgo para una nación si la infraestructura es atacada, especialmente, infraestructuras que dependen de sistemas de información y comunicaciones. En consecuencia, y bajo la lógica de la intercomunicación en el ciberespacio, existen responsabilidades de ciberdefensa y ciberseguridad que son transversales, por tanto, las capacidades operacionales de la guerra deben identificar y contrarrestar los diferentes riesgos y amenazas en los diferentes campos civiles y militares.

El sexto capítulo, *El Derecho Internacional como marco regulatorio de la ciberguerra*, y sin dejar de lado el marco jurídico, este apartado aborda el alcance jurídico que debe desarrollarse mediante políticas y marcos regulatorios internacionales enfocados al ciberespacio. Demostrando la existencia jurídica de regular el enfrentamiento o conflicto desde un nuevo escenario de guerra. Se resalta las bases generadas en el *Manual de Tallínn*, afirmando que pueden ser insumos para considerar el derecho de defensa de un Estado ante ciberataques.

Finalmente, el capítulo *Desafíos para afrontar la ciberguerra Equipo CEEAG*, este apartado aborda el debate sobre los desafíos a afrontar a largo plazo por parte de los Estados. Se establece que existen ejes fundamentales que deben desarrollarse para contener las amenazas, los riesgos del ciberespacio y se encuentran enmarcadas en competencias, capacidades y nivel madurez de los sistemas de información y organizacionales para generar respuesta ante incidentes. Si bien todos los riesgos o amenazas pueden afectar la infraestructura crítica, lo que se aconseja es generar respuestas inmediatas ante ataques y protocolos preventivos ante amenazas que pueden resultar comunes.

Autora de la reseña

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

Referencias

Villagra R., Díaz H., Leiva R., Arteaga M., Marowski C., y Polloni M. (2018). *La ciberseguridad, sus impactos y desafíos*. Centro de Estudios Estratégicos.


EDITORIAL ESDEG

Revista **Ciberespacio, Tecnología e Innovación**

EDITORIAL **ESDEG**

ISNN 2955-0270

9 772955 027005