EDITORIAL ESDEG

Revista
Ciberespacio, Tecnología e Innovación
Volumen 1, número 2, julio-diciembre 2022
Bogotá, D.C, Colombia
ISSN: 2955-0270 • eISSN: 3028-3310
Página web: https://esdegrevistas.edu.co/index.php/rcit

El Ciberespacio como escenario para enfrentar los delitos transnacionales en Colombia

Cyberspace as a scenario to confront transnational crimes in Colombia

Eduardo Velandia Becerra

CITACIÓN APA:

Velandia Becerra, E. (2022). El Ciberespacio como escenario para enfrentar los delitos transnacionales en Colombia. *Ciberespacio, Tecnología e Innovación, 1*(2), 167-178. https://doi.org/10.25062/2955-0270.4769

Publicado en línea: **Diciembre 30 de 2022**

Enviar un artículo a la Revista

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

Revista Ciberespacio, Tecnología e Innovación
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.

CC BY NC ND

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