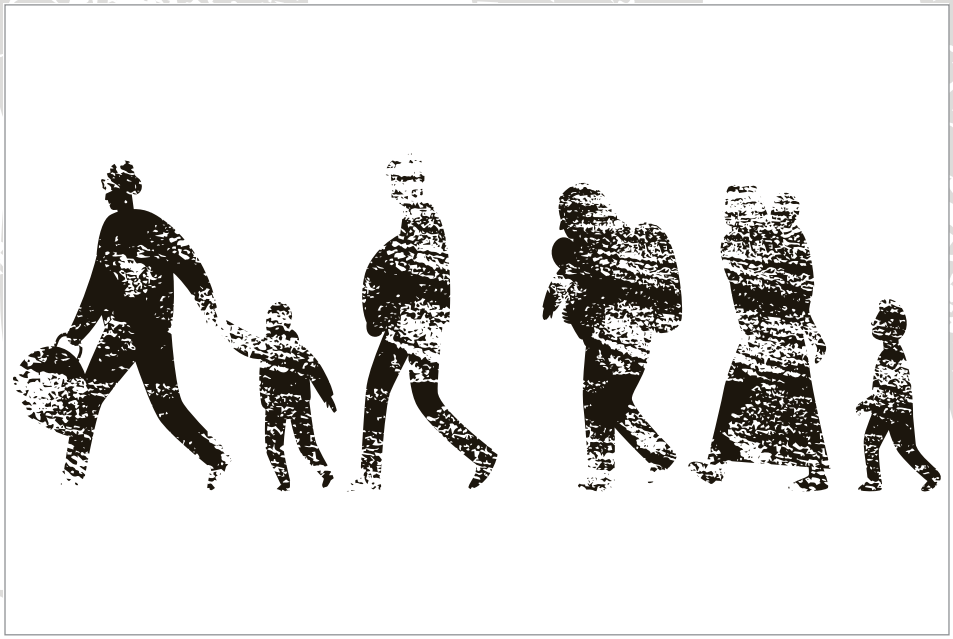
Desafíos de la seguridad humana en los nuevos dominios de la guerra

Cómo citar este artículo [Chicago]: Cano Cuevas, Diego Fernando. "Desafíos de la seguridad humana en los nuevos dominios de la guerra". *Novum Jus 18*, núm. 3 (2024): 41-68. https://doi.org/10.14718/NovumJus.2024.18.3.2

Diego Fernando Cano Cuevas



Código: 1393938668 • Autor: istockphoto.com

https://doi.org/10.14718/NovumJus.2024.18.3.2

Desafíos de la seguridad humana en los nuevos dominios de la guerra

Diego Fernando Cano Cuevas*
Escuela Superior de Guerra General Rafael Reyes Prieto

Recibido: 10 de septiembre de 2023 **| Evaluado:** 11 de marzo de 2024 **| Aceptado:** 4 de abril de 2024

Resumen

El presente documento examina los nuevos dominios de la guerra y los desafíos que plantean a la seguridad humana en la era moderna. En particular, se analiza el ciberespacio, las operaciones de información y la militarización del espacio exterior como dominios emergentes que requieren una atención estratégica y una política adecuada. En primer lugar, se aborda el ciberespacio como un dominio crítico. El crecimiento exponencial de la conectividad digital ha dado lugar a una mayor vulnerabilidad a los ciberataques, arriesgando la seguridad e intimidad de las personas. Proteger los datos de cada persona y la infraestructura digital se vuelve esencial para salvaguardar la seguridad humana. En segundo lugar, se exploran las operaciones de información como un desafío importante. La propagación de desinformación puede disminuir la confianza en las instituciones y generar polarización en la sociedad; por eso, se prioriza enseñar sobre medios y pensamiento crítico para contrarrestar estas amenazas a la seguridad humana. Por último, se analiza la militarización del espacio exterior como un nuevo dominio de guerra: actividades militares en el espacio como la vigilancia y el desarrollo de armas antisatélite plantean riesgos significativos para la seguridad y la estabilidad mundial. La comprensión de estos desafíos y el desarrollo de políticas efectivas son cruciales para proteger la seguridad de las personas y sus derechos. El abordaje integral de estos desafíos es esencial para garantizar el bienestar de cada ser humano en un mundo que cada día depende más de la cibernética y la tecnología.

Palabras clave: dominios de la guerra; seguridad humana; ciberespacio; operaciones de información; militarización del espacio exterior; desafíos de seguridad.

* Mayor (R) del Ejército Nacional de Colombia. Magíster en Estrategia y Geopolítica, Escuela Superior de Guerra General Rafael Reyes Prieto. Profesional en relaciones internacionales y estudios políticos, Universidad Militar Nueva Granada. Profesional en Ciencias Militares, Escuela Militar de Cadetes General José María Córdova. Docente, Escuela Superior de Guerra General Rafael Reyes Prieto. Correo electrónico: diego.cano@esdeg.edu.co. ORCID: https://orcid.org/0000-0002-8317-8845

https://doi.org/10.14718/NovumJus.2024.18.3.2

Challenges to Human Security in the New Domains of Warfare.

Diego Fernando Cano Cuevas*
Escuela Superior de Guerra General Rafael Reyes Prieto

Received: September 10, 2023 **| Evaluated:** March 11, 2024 **| Accepted:** April 04, 2024

Abstract

This paper examines the new domains of warfare and the challenges they pose to human security in the modern era. Specifically, it discusses cyberspace, information operations, and the militarization of outer space as emerging domains that require strategic attention and an appropriate policy. First, cyberspace is addressed as a critical domain. The exponential growth of digital connectivity has resulted in increased vulnerability to cyber-attacks, risking the security and privacy of individuals. Protecting individual data and digital infrastructure becomes essential to safeguard human security. Second, information operations are explored as a major challenge. The spread of disinformation can erode trust in institutions and foster polarization in society; therefore, teaching about media and critical thinking is prioritized to counter these threats to human security. Finally, the militarization of outer space is analyzed as a new domain of warfare. Military activities in space, such as surveillance and the development of anti-satellite weapons, pose significant risks to global security and stability. Understanding these challenges and developing effective policies are crucial to protecting the security of individuals and their rights. A comprehensive approach to addressing these challenges is essential to ensure the well-being of every human being in a world that is becoming ever more reliant on cybernetics and technology.

Keywords: domains of warfare; human security; cyberspace; information operations; militarization of outer space; security challenges.

Introducción

En el contexto militar un *dominio de guerra* se refiere a una área en la que se llevan a cabo las operaciones militares y donde los actores involucrados intentan obtener ventaja sobre sus adversarios. Históricamente, estos espacios se han definido por el medio físico en el que se desarrollan: el dominio terrestre, marítimo, aéreo y el espacial. Sin embargo, últimamente surge un debate sobre la necesidad de reconocer y abordar nuevos escenarios de confrontaciones, evidentes por los avances tecnológicos y la creciente interconexión de sistemas, especialmente en lo que se refiere al uso y control de información y tecnología, dado el papel crítico que aquellos avances desempeñan en los conflictos contemporáneos.

Esta modificación en los recursos y estrategias de guerra traspasa las fronteras geográficas, llegando a los "nuevos dominios" que trascienden los límites físicos. Varios autores han abordado el tema y su importancia en el contexto contemporáneo. Entre ellos, se encuentra William J. Lynn III, quien describe ampliamente los desafíos de la ciberseguridad y la guerra cibernética[1]. Asimismo, Martin Libicki se ha enfocado en el estudio de la ciber estrategia y la ciberdefensa[2]. Se suman John Arquilla y David Ronfeldt, quienes a través de la Rand Corporation escribieron un artículo en el cual exploran la idea de la guerra en el ciberespacio y las implicaciones que tiene[3].

Otros pensamientos de teóricos se orientan a la tecnología y su influencia sobre la forma y el lugar donde se hace la guerra. Por ejemplo, Richard A. Clarke y Robert K. Knake analizan la creciente amenaza de la guerra cibernética y las implicaciones de la militarización del espacio exterior[4]. David S. Alberts y Richard E. Hayes discuten cómo las nuevas tecnologías están cambiando la naturaleza de los dominios de guerra tradicionales y están dando lugar a nuevos espacios en donde las operaciones de información y desinformación están presentes de primera mano[5]. Por último, es necesario destacar a Thomas Rid, quien examina el papel de la desinformación y la guerra de información en los conflictos modernos[6].

---

1 William J. Lynn III, "A Military Strategy for the New Space Environment", *The Washington Quarterly* 34, núm. 3 (2011): 9.

2 Martin Libicki, *Cyberdeterrence and Cyberwar*, 1a ed. (Santa Monica, CA: RAND Corporation, 2009), 240.

3 John Arquilla y David Ronfeldt, "Cyberwar is coming!", en *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla y David Ronfeldt (Santa Monica, CA: RAND Corporation, 1997), 23-60.

4 Richard A. Clarke y Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (Madrid: Ecco, 2011), 320.

5 David S. Alberts y Richard E. Hayes, *Power to the edge: Command... control... in the information age* (Washington, D.C.: Command and Control Research Prosinegram [CCRP], 2003), 303.

6 Thomas Rid, *Active measures: The secret history of disinformation and political warfare*, 1ra. edición (New York: Farrar, Straus, and Giroux, 2020), 513.

Estos son solo algunos ejemplos de los autores que han contribuido al debate y análisis de los nuevos dominios de guerra. Cabe destacar que en la lista hay otros expertos y académicos que han realizado aportes en este campo. No obstante, se ha observado que este cambio en los estudios sobre los dominios de la guerra se ha centrado en una creciente atención sobre el ciberespacio, el manejo de la información y el espacio exterior.

Estos nuevos puntos de análisis han tomado importancia en el panorama global, en especial en la seguridad y defensa. El ciberespacio, capaz de influir en sistemas críticos y desencadenar impactos devastadores, es un entorno en el que se presentan las confrontaciones entre los Estados y donde actores no estatales compiten por el control y la supremacía. Las operaciones de información, por su parte, abarcan desde la manipulación de noticias y desinformación hasta la ciber-propaganda y la guerra psicológica, pretendiendo moldear percepciones y obtener ventajas estratégicas. Además, el creciente número de países y entidades que lanzan satélites y desarrollan capacidades militares en órbita ha generado una campo de batalla diferente en el que existen desafíos y riesgos para la seguridad nacional. Este contexto, en constante evolución, muestra que el estudio de estos dominios emergentes es ineludible para comprender las dinámicas e implicaciones estratégicas de los conflictos contemporáneos.

A esta evolución se suma el Informe de Desarrollo Humano del Programa de las Naciones Unidas para el Desarrollo (PNUD) de 1994, que cambia el paradigma de la *seguridad*, al llevarla desde la protección de los intereses de un Estado hasta la defensa del ser humano. Con esto, da paso al concepto de *seguridad humana*, que otorga mayor importancia al ser humano, si se tiene en cuenta que este tipo de seguridad puede orientarse para lograr de manera más efectiva la protección de las personas frente a la violencia, en lo concerniente a los derechos humanos, y para satisfacer las carencias propias del ser humano[7], recogiendo el concepto de "dividendo de paz" y asegurando que los recursos no se destinen únicamente a la ejecución de planes bélicos. Desde esta perspectiva, los programas de seguridad también deben apoyar frente a amenazas crónicas y súbitas que pudiesen afectar a las personas en ámbitos como la salud, la economía, el medio ambiente, la seguridad personal, la vida en comunidad, la seguridad alimentaria y la política[8].

[7] Jorge Carvajal, "Seguridad Humana, en el contexto de la lucha contra el terrorismo", *Novum Jus* 2, núm. 1 (2008): 205-234.

[8] Christian Acevedo, Valentina Ballesteros y María Antonieta Corcione, "Seguridad humana y seguridad multidimensional, su enfoque y utilidad para proteger los derechos humanos [en línea]", *Revista Científica General José María Córdova* 20, núm. 40 (2022): 1106.

El propósito del informe era influir en el resultado de la Cumbre de Copenhague en 1995. Por eso, la seguridad humana se planteó como un ejercicio con fines estratégicos[9].

Ahora bien, si se compara la definición de seguridad humana con la importancia del ciberespacio, las operaciones de información y el espacio exterior como nuevos dominios de la guerra, se encuentra que los desafíos planteados son significativos para la seguridad humana en la actualidad, como ámbitos que representan una ampliación de los medios de conflicto y amenazas diferentes de los tradicionales. El ciberespacio ofrece una plataforma para ataques cibernéticos que comprometen infraestructuras críticas, sistemas financieros y la privacidad de las personas. Las operaciones de información, a través de la manipulación de noticias y la propagación de desinformación, tienen el potencial de socavar la confianza pública, polarizar sociedades y debilitar la gobernabilidad.

Además, el espacio exterior se ha convertido en un escenario donde las capacidades militares pueden ser desplegadas y producir inquietud sobre el uso de armas espaciales y posibles conflictos en el espacio. Enfrentar estos desafíos requiere comprender las nuevas dinámicas de guerra y una cooperación global efectiva para desarrollar estrategias fortalecedoras de la seguridad humana en un mundo vinculado por las redes y tecnológicamente dependiente, en el cual se ponen en riesgo los derechos fundamentales y, con ellos, la privacidad y el bienestar de las personas en la era digital. Si la seguridad humana debe incluir la ciberseguridad, en el entendido de que un nuevo dominio de la guerra es el espacio cibernético, se puede comprender la tesis de Sánchez, quien postula la seguridad en el espacio cibernético como un derecho ciudadano y un deber del Estado[10].

En síntesis, el avance de la tecnología sumado a la desarrollo de la guerra han dado lugar a nuevos entornos de conflicto que desafían la seguridad humana. La ciberguerra, la guerra de la información y la militarización del espacio son ejemplos donde la interconexión global y la dependencia de la tecnología han transformado la naturaleza de la seguridad y sus implicaciones para los individuos y las sociedades[11].

9 Keith Krause, "Seguridad humana: ¿ha alcanzado su momento?", *Papeles de cuestiones internacionales*, núm. 90 (2005): 19-29.

10 Marco Sánchez, "La inteligencia artificial en el sector público y su límite respecto de los derechos fundamentales", *Estudios Constitucionales* 20, núm 2 (2022): 257-284.

11 Vicente Torrijos y Daniel Jiménez, "Tendencias en el estudio de la seguridad en un quinto dominio de la guerra", *Cuadernos de la Guardia Civil. Revista de Seguridad Pública*, núm. 65 (2021): 73-92.

En este texto se examinan las amenazas a la seguridad humana en los nuevos dominios de la hostilidad, enfocándose en tres áreas: el ciberespacio, la guerra de la información y la militarización del espacio exterior. Todos presentan riesgos y amenazas que requieren comprensión y estrategias de respuesta efectivas.

Inicialmente, se explora el ciberespacio, donde los ataques y la ciberguerra son una amenaza para la infraestructura crítica, robo de información y pérdida de privacidad. Se analiza la transformación de la seguridad en lo que respecta a sistemas informáticos y datos personales en desafíos en un mundo interconectado[12]. Después, se analiza el dominio de la guerra desde la información, evaluando el rol que desempeñan las redes sociales y medios de comunicación en ella y cómo afecta la seguridad humana en términos de confianza y toma de decisiones informadas[13].

Finalmente, se estudia la militarización del espacio exterior, donde la competencia por el control y acceso a los activos espaciales plantea desafíos para la seguridad humana mundialmente. Se describen las implicaciones de la destrucción de satélites, la interrupción de las comunicaciones y la navegación por GPS, así como las preocupaciones éticas y humanitarias asociadas con el desarrollo de armas autónomas y sistemas de inteligencia artificial en el espacio[14].

Este análisis se guía con el prototipo liberal aplicado en las relaciones internacionales, entendiendo que los nuevos dominios de la guerra han generado desafíos para la seguridad humana, por lo que se propone explorar estos desafíos en el espacio cibernético, donde las confrontaciones se dan por el manejo de la información y la militarización del espacio exterior, destacando la necesidad de enfoques integrales y cooperación internacional que garanticen la defensa de los derechos fundamentales de los seres humanos en este nuevo escenario.

La perspectiva de la teoría liberal a la vista de la seguridad humana y los nuevos dominios de la guerra

El liberalismo en las relaciones internacionales desempeña un rol trascendental en la cooperación internacional y la exploración de procedimientos con los que de forma

[12] Sierra-Zamora, P. A. y A. Castaño-Bedoya, "Guerras híbridas, irrestrictas, asimétricas y jurídicas en el nuevo orden mundial", *Revista Científica General José María Córdova* 20, núm. 40 (2022): 852-869.

[13] Manuel Torres Soriano, "Operaciones de influencia vs. desinformación: diferencias y puntos de conexión", *Documento de Opinión IEEE*, núm. 64 (2022): 16.

[14] Javier Jordán Enamorado, "Competición entre grandes potencias y militarización del espacio exterior", *Araucaria*, núm. 53 (mayo 2023): 169-194.

colectiva se solucionen los retos globales. En el contexto de los nuevos dominios de la guerra, donde la seguridad humana está en juego, el enfoque liberal destaca la importancia de la cooperación y el establecimiento de cánones internacionales para garantizar la protección de los individuos y las sociedades[15].

Desde la perspectiva liberal, los desafíos de seguridad humana en los nuevos dominios requieren una respuesta cooperativa y multilateral, que deje de lado la mentalidad de "suma cero", buscando intereses comunes y la creación de acuerdos que beneficien a todas las partes involucradas[16].

Para David Charles-Philippe y Raúl Quiroz, en la ciberguerra, el enfoque liberal resalta la importancia de desarrollar normas y regulaciones internacionales que aborden los desafíos emergentes, forjando la intervención activa de actores que hacen o no parte del Estado en la formulación de políticas y de instrumentos de cooperación que promuevan una cultura anticorrupción, la responsabilidad y la confianza mutua[17].

La cooperación internacional basada en los principios liberales también se centra prevenir conflictos y solucionarlos pacíficamente evitando la confrontación y la escalada militar, promoviendo la negociación y la mediación como herramientas para enfrentar las tensiones y resolver los conflictos en los nuevos dominios de la guerra[18]. El enfoque liberal destaca la importancia de fortalecer las instituciones internacionales para abordar efectivamente los desafíos de seguridad humana en un escenario diferente[19]. Estas instituciones son un puente para promover la coordinación y ejecución de mejores prácticas entre los Estados y otros actores relevantes.

El enfoque liberal y la cooperación internacional son la guía para el desarrollo de esta investigación, porque fundamentan la comprensión de los desafíos de seguridad humana en los nuevos dominios de la guerra, la promoción de la cooperación,

15 Matias Ilivitzky, "Debates actuales sobre el orden liberal internacional", *Comillas Journal of International Relations*, núm. 24 (2022): 35-51.

16 Karlos Pérez de Armiño, "El concepto y el uso de la seguridad humana: análisis crítico de sus potencialidades y riesgos", *Revista CIDOB d'Afers Internacionals*, núm. 76 (2006): 59-77.

17 Charles Philippe David y Raúl Quiroz, eds., *La Guerra y la Paz: Enfoque Contemporáneo Sobre la Seguridad y la Estrategia* (Barcelona: ICARIA, 2008), 17-26.

18 Rafael Grasa Hernández, "Vínculos entre seguridad, paz y desarrollo: evolución de la seguridad humana: de la teoría al programa político y la operacionalización", *Revista CIDOB d'Afers Internacionals*, núm. 76 (2006): 9-46.

19 Jorge Ulloa Plaza y María Angélica Benavides Casals. "Moralidad, guerra y derecho internacional. Tres cuerdas para un mismo trompo: la humanidad". *Novum Jus* 17, núm. 1 (2023): 259-282.

el desarrollo de normas internacionales y el fortalecimiento de las instituciones, variables esenciales para garantizar la protección de los derechos fundamentales y la seguridad de las personas en la evolución de la guerra.

Métodos

La metodología tiene un enfoque cualitativo-hermenéutico, para interpretar la impresión de los nuevos dominios de la guerra en la seguridad humana. Según Beuchot, la hermenéutica analógica se define como los parámetros bajo los que se interpretan los problemas que aquejan a la sociedad contemporánea[20]. En la comprensión del vínculo existente entre la seguridad humana y hechos con los cuales interactúa de cara a los nuevos dominios de la guerra, esta hermenéutica ayuda en el reconocimiento de la sociedad de la que hace parte[21]. Frente a los conceptos de los nuevos dominios de la guerra y su relación con la seguridad humana, la analogía es una herramienta útil para obtener resultados y explica dos tipos de interpretaciones extremas entre las que media la analogía: la unívoca y la equívoca[22].

Para seleccionar los textos que conformarán el *corpus* de análisis, se tiene en cuenta las siguientes palabras clave: dominios de la guerra y seguridad humana. Como criterios de inclusión, se priorizan artículos resultados de investigación, informes de universidades o entidades gubernamentales internacionales sobre estrategia y seguridad, idioma y periodo de tiempo (2010-2022), así como motores de búsqueda dentro de los que se incluyen Dialnet, EBSCO, Google Académico, Science Direct, SciELO, Proquest. Los criterios de exclusión tienen en cuenta variables y características que demuestren que los documentos corresponden a trabajos de grado para optar a títulos de maestrías o doctorados, también material gris.

Se llevaron a cabo diversas etapas dentro del marco de la hermenéutica analógica. En primer lugar, se abordó la fase sintáctica, donde se exploraron los conceptos de contracción univocista (U) y expansión equivocista (E), empleando categorías de análisis vinculadas a los ámbitos de la guerra y la seguridad humana. Estas categorías sirvieron como base para organizar la información recopilada durante la investigación. Luego, el momento semántico se encargó de determinar y analizar las posturas univocistas (U1-5) y equivocistas (E1-5) con respecto a la relación

[20] Mauricio Beuchot, *Hechos e interpretaciones: Hacia una hermenéutica analógica* (México D.F.: Fondo de Cultura Económica, 2016), 114.
[21] Beuchot, *Hechos e interpretaciones*, p. 112.
[22] Beuchot, *Hechos e interpretaciones*, p. 112.

entre seguridad humana y los ámbitos de la guerra. Por último, la fase pragmática estableció una analogía (F) entre los aspectos unívocos y equívocos de las variables asociadas a los desafíos que enfrenta la seguridad humana en el ciberespacio, las operaciones de información y la militarización del espacio exterior.

Resultados obtenidos

Últimamente, la noción de *guerra* ha cambiado significativamente, incluyendo nuevos espacios en donde los conflictos pueden desarrollarse. Estos son el resultado de avances tecnológicos y reformas en las formas de interacción y comunicación de la sociedad. Tradicionalmente, las operaciones militares hacían parte de un marco operacional-estratégico orientado a amenazas en los dominios de la guerra tradicionales: el dominio terrestre (ejército), el marítimo (fuerzas navales) y el aéreo (fuerzas aéreas).

El desarrollo de las acciones militares era resultado de la combinación de estrategias, tácticas y técnicas en dominios diferenciados. No obstante, la mutación de los conflictos armados es rápida; por ejemplo, la invasión de Rusia en Ucrania o el actuar de grupos terroristas islamistas son la justificación para modificar la forma de afrontar las operaciones en los dominios tradicionales y nuevos, lo que muestra la importancia de desarrollar estrategias y capacidades para enfrentar los desafíos emergentes y mantener la superioridad en el campo de batalla. Ignorar los nuevos dominios podría generar desventaja y vulnerabilidad frente a ataques o manipulación por parte de los adversarios.

Una vez realizado el estudio de hermenéutica analógica, se evidencia que uno de los enfoques destacados es la trilogía compuesta por el ciberespacio, las operaciones de información y la militarización del espacio exterior. Estos se consideran críticos por su capacidad para influir en las percepciones, las capacidades militares y la seguridad nacional.

En el espacio cibernético, Martin Libicki explora la naturaleza de la guerra cibernética y la importancia de la ciberseguridad en la era digital; ante la seguridad humana representan un desafío del que los Estados deben protegerse y proteger a las personas de las amenazas que traen consigo[23]. Por su parte, William J. Lynn III examina los desafíos de la ciberseguridad y su impacto en la estrategia militar, donde la seguridad humana es el escenario estratégico[24].

[23] Libicki, *Cyberdeterrence and Cyberwar*, 240.
[24] Lynn III, "A Military Strategy", 9.

Para las operaciones de información, Thomas Rid investiga el papel de la desinformación y la guerra de información en los conflictos modernos[25]; Richard A. Clarke y Robert K. Knake analizan la amenaza de la guerra cibernética que influye en la seguridad nacional[26]; en cuanto a la militarización del espacio exterior, David S. Alberts y Richard E. Hayes exploran las trasformaciones que forja la tecnología espacial en la naturaleza de los dominios de las confrontaciones tradicionales[27].

Ciberespacio: conceptualización y su relación con la ciber-guerra

El *ciberespacio* es el ámbito virtual en el que las redes de computadoras interconectadas operan. Aquí, los actores desarrollan actividades como el espionaje, la infiltración de sistemas, la sustracción de la información y la paralización de infraestructuras críticas, convirtiéndose en una preocupación creciente por las vulnerabilidades que son usadas para lograr sus objetivos estratégicos[28]. En la actualidad, el ciberespacio es un entorno que impulsa el desarrollo social; sin embargo, han surgido desafíos significativos en términos de seguridad que a través del ciberespacio amenazan con nuevos escenarios y formas de conflicto[29].

Infraestructura crítica bajo amenaza

La infraestructura crítica hace referencia a los sistemas eléctricos, las redes de transporte y las comunicaciones que son vulnerables ante ataques cibernéticos que generan caos y afectan la vida diaria de las personas[30]. Por eso, su preservación es priorizada por los gobiernos y organizaciones que implementan medidas de seguridad para responder rápidamente a los posibles ataques.

Existen otras estructuras críticas bajo amenaza. Estas incluyen los computadores y sistemas que guardan información importante y son atacados[31]; por ejemplo, Singer y Friedman hablan sobre un ataque sufrido por un gobernante sirio en 2006

25 Rid, "Active measures", 513.
26 Clarke y Knake, *Cyber War*, 320.
27 Alberts y Hayes, *Power to the edge*, 303.
28 Hevert Molina Losada, "El ciberespacio un escenario moderno para los sistemas de seguridad" (Tesis de especialización en Administración de Seguridad, Universidad Militar Nueva Granada, 2017), 24.
29 Rafael Rodríguez, "¿Qué seguridad? Riesgos y amenazas de internet en la seguridad humana", *Araucaria* 18¸ núm. 36 (2016): 391-415.
30 Elena García, "Altas tecnologías, conflictos armados y seguridad humana", *Araucaria* 18, núm. 36 (2016): 265-293.
31 Jairo Becerra Ortiz *et al.*, "Implicaciones jurídicas en el entorno del *big data*: el caso del app Navega Seguro". *Novum Jus* 17, núm. 1 (2023): 357-388.

mientras paseaba por Londres, cuando los israelíes irrumpieron en su habitación e instalaron un troyano en su computador, que les dio acceso a una foto en la que aparecía uno de los lideres del programa nuclear de Corea del Norte y el jefe de la Comisión de Energía Atómica de Siria, lo que generó alarma en el mundo[32].

Lo anterior demuestra que los datos informáticos y los sistemas en donde están almacenados también son parte de la infraestructura crítica vulnerable que se ubica en teléfonos móviles, redes sociales y redes de computadores a las que se accede por plataformas de *streaming*. Un ataque dirigido a alguna de ellas deja consecuencias que pueden tener un alcance mayor en temas políticos y en el desarrollo de la sociedad[33].

La era digital ha dado paso a dinámicas diferentes en procesos sociopolíticos y económicos. También ha abierto un espacio para el robo de información y la violación de la privacidad con ataques cibernéticos dirigidos a empresas, organizaciones gubernamentales y usuarios que posteriormente son víctimas de la exposición de datos confidenciales y personales, lo que da lugar a inquietudes que se vinculan con la seguridad de la información y la salvaguarda de los datos.

Desafíos en un mundo interconectado

Los desafíos se enmarcan en la dependencia de la tecnología y los sistemas informáticos. Esta hace que las personas sean más susceptibles a los ataques cibernéticos, al convertirlas en potenciales víctimas de robo de identidad o extorsión con el acceso a sus datos financieros o de salud[34]. A este desafío se suma el de la complejidad de los sistemas empleados por *hackers* y actores malintencionados que se infiltran en sistemas y redes sin ser percibidos, lo que impide atribuir responsabilidades a los perpetradores de los ataques cibernéticos; por eso, pueden ocultar su identidad y ubicación. Esta falta de atribución limita la aplicación de la ley, contribuye a la impunidad y alienta a otros a realizar acciones similares, lo que genera un entorno inseguro para las personas[35].

[32] P.W. Singer y Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014), 320.

[33] L. Bowers, "Safewards: un nuevo modelo de conflicto y contención en salas psiquiátricas", *Revista de enfermería psiquiátrica y de salud mental* 21, núm. 6 (2014): 499-508.

[34] Eduardo Diniz, "Tecnologías de back-office: desafíos no mundo interconectado", en *Administração Bancária: uma visão aplicada* (Rio de Janeiro: Editora FGV, 2014), 177-200.

[35] Ilivitzky, "Debates actuales", 35-51.

Esta transgresión hace pertinente consolidar la seguridad humana y los derechos fundamentales ante los desafíos en el ciberespacio, demostrando que las circunstancias relacionadas con este requieren de tácticas de seguridad efectivas en contra de las amenazas que provienen de actores que pueden ser clasificados como parte del Estado o no estatales. Dichos actores tienen a veces un alcance trasnacional que obliga a pensar en el ejercicio de la cooperación internacional y en herramientas para fortalecer la seguridad en el ciberespacio que se complementan con la intervención de los ámbitos gubernamental, empresarial y el de la comunidad civil[36].

En la actualidad, todas las circunstancias relacionadas con el ciberespacio, incluyendo la ciberguerra, los ataques cibernéticos, el robo de información y la pérdida de privacidad, afectan la seguridad humana y representan una amenaza para las personas[37], porque la interconexión global crea vulnerabilidades que hacen que los ataques en el ciberespacio se propaguen rápidamente a través de redes que afectan a individuos y organizaciones en poco tiempo[38].

Guerra de la información

Con el surgimiento de las redes sociales, y con la tendencia enfocada en digitalizar los medios de comunicación, la difusión de información falsa se ha forjado una confrontación para minimizar a los adversarios y promover sus intereses. Esto ha mostrado que la contienda librada por la información implica el uso estratégico de comunicación y la propaganda para persuadir a la opinión pública sobre la imagen de instituciones y manipular su percepción de la realidad.

En la sociedad de la era digital, la guerra de la información ha emergido como una prueba crítica para la estabilidad y la seguridad de la sociedad que al mismo tiempo la divide, demostrando el poder de quien posee la información, ya que la estrategia promueve el uso estratégico de esta para lograr objetivos políticos, económicos o ideológicos. Es así como actores del Estado y no estatales ejecutan acciones basadas en noticias falsas y datos equivocados que posteriormente difunden y con los que manipulan a los ciudadanos, generando confusión y dudas para perturbar la

[36] Ángel Barbas, "Educomunicación; desarrollo, enfoques y desafíos en un mundo interconectado", *Foro de Educación*, núm. 14 (2012): 157-175.

[37] Antonio Martín, "Ciudadanía global. Un estudio sobre las identidades sociopolíticas en un mundo interconectado", *ARBOR Ciencia, Pensamiento y Cultura* 193, núm. 786 (2017): 14.

[38] Bernardo Marques y Marcelo Quiroga, "La Cuarta Revolución Industrial y los impactos de un mundo interconectado, en la libertad, seguridad e intimidad", *Derecho y Cambio Social*, núm. 55 (2019): 238-273.

percepción de la realidad y debilitar la cohesión social, fomentando la polarización e interviniendo en los factores que importan al influir en las decisiones de los ciudadanos, todo lo cual resulta minando la democracia.

Según Jorge de Esteban, la prensa se constituye de los medios de comunicación que se dirigen y cubren a la mayoría de la población; por lo tanto, es el instrumento democrático de la libertad para acceder a información real, influyendo en el control del poder político[39]. Por eso Burke la identifica como el "cuarto poder" que complementa los poderes del Estado de Montesquieu; sin embargo, los medios de comunicación pueden actuar de dos formas: o bien aplicando propaganda sobre información real, o bien informando, controlando y denunciando los abusos del poder político.

Este nuevo escenario requiere de tareas para el Estado en ámbitos como las operaciones de información, operaciones psicológicas y comunicaciones estratégicas, necesarias para enfrentar la guerra jurídica y mediática que se suscita frecuentemente ante el desarrollo de la actuaciones de la Fuerza Pública. Esto se aprecia, por ejemplo, en operaciones militares donde existe información que oculta al adversario; también en operaciones de información donde se planean, coordinan y sincronizan las capacidades centrales (guerra electrónica, operaciones de redes computarizadas, operaciones sicológicas, operaciones militares de decepción y operaciones de seguridad), secundarias (certeza de información, seguridad física, ataque físico, contraespionaje y camarógrafo de combate) y relativas (operaciones civiles-militares, o aquellas que fortalecen la salvaguardia de la diplomacia pública), para atentar o defender con información los objetivos militares, políticos o legales.

Por lo tanto, la *guerra informática* se relaciona con el manejo de la información en favor de los objetivos nacionales y la información es la representación del poder nacional que favorece los factores diplomáticos, la competitividad en la economía, además del aprovechamiento eficaz de las habilidades y recursos de las fuerzas militares. Con ello se muestra que esta confrontación entre naciones, o entre grupos que hacen parte de la sociedad contemporánea, utiliza los medios informativos que hacen parte del ciberespacio y en donde es probable que ocurra un futuro conflicto estratégico.

[39] Jorge De Esteban, "Los medios de comunicación como control de poder político", *Revista de Derecho Político*, núm. 42 (1997): 11-34.

Esta guerra de la información transforma la manera en la que se dirige en nivel operacional, así como las actividades militares. También es el espacio donde se llevan a cabo acciones que distan de las que caracterizan una guerra cuando se trata de defender la seguridad sin las fuerzas militares, con lo cual se expone un modo de hacer la guerra donde el blanco es la mente humana que toma decisiones clave frente a la paz, el ámbito militar, los elementos y facultades incluidas en sus estructuras estratégicas.

Frente a este tipo de conflicto, Stein indica que la guerra de información es el ámbito donde convergen ideas y palabras altisonantes que indican al ser humano la manera en que "debería" pensar, mostrando que su objetivo está en los seres humanos y sus decisiones[40]. En la realidad, involucra a medios de comunicación masiva que difunden un mensaje específico y creado para la audiencia que se quiere persuadir, lo que resulta forjando una guerra psicológica con la que se aterroriza al enemigo y a la población civil.

Lo anterior hace parte de las operaciones psicológicas (PsyOps) relacionadas con el intercambio de información y las relaciones públicas, pero no con la psicología. Dichas operaciones se valen del trabajo de un publicista que aplica la fórmula clauswitziana basada en la propaganda de guerra como una forma de continuar la propaganda política, utilizando otros instrumentos. Por eso, Pizarroso indica que la *propaganda* no es más que la acción que forja la violencia mental para obligar a una persona a someterse a la voluntad de otra[41], lo que Bisky explica desde la escuela marxista alemana como el uso de la persuasión (Überredung), inscrita en la investigación comunicacional o comunicación persuasiva, importante en operaciones contra el oponente, que busca disminuir la moral y eficiencia, evitar las deserciones minimizando la influencia de su propaganda y consiguiendo la colaboración de la población civil[42].

Alfonso Bauluz afirma que esta guerra establece las características de la política que la guía: la manipulación informativa, el discurso político y la posibilidad de la desaparición del periodismo neutral, sin tentativas políticas que sean vistas como

40 George Stein, "La Guerra de Información", *Air & Space Power Journal*, en línea (1996).

41 Alejandro Pizarroso, "Aspectos de propaganda de guerra en los conflictos armados más recientes", *Redes.com*, núm. 5 (2009): 49-65.

42 Lothar Bisky, *Crítica de la Teoría Burguesa de la Comunicación de Masas* (Madrid: Ediciones de la Torre, 1982), 222.

un ejercicio profesional importante para mantener las democracias del siglo XXI[43]. Ante esto, Javier Jaspe indica que las operaciones de información son importantes para influir en determinados sucesos, al favorecer ideas políticas y facilitar la intervención de algunos actores, mostrando estas acciones como parte favorable de la estrategia comunicativa y aprovechándose de una situación desfavorable para obtener un beneficio estratégico[44].

En lo relativo a la información, Snegovaya considera que con la propaganda se logra ejercer un control reflexivo sobre la población, como sucede en el caso de Rusia donde se desarrolla una guerra híbrida complementada con una guerra informativa disfrazada de control reflexivo que lleva al oponente a actuar en favor de Rusia desde una percepción manipulada de la situación[45].

En la actualidad, los Estados basan sus actividades de comunicación en herramientas como X, antiguo Twitter, donde es posible difundir un mensaje en tiempo real, desde perfiles verificados y con un mayor alcance, lo que Kington explica diciendo que esta red es un altavoz ideológico, un tablón de anuncios y el espacio de comunicación de autoridades religiosas[46].

Es esta capacidad de alcance y difusión lo que lleva a pensar en combatir la problemática del crimen trasnacional desde la cooperación internacional, como lo confirma Linares cuando dice que las redes criminales son un reto desde la perspectiva jurisdiccional y de las diferencias legales entre Naciones. Por eso, según Linares, es importante que las operaciones multilaterales se basen en instrumentos internacionales como los propuestos por la Convención de Palermo en el 2000; de esta manera es posible que los países implementen leyes con las que puedan asignar responsabilidades a los promotores de la guerra de la información y de actividades ilícitas derivadas que afecten la seguridad mundial[47].

---

43 Alfonso Bauluz, *Prensa y manipulación. El Pentágono y las Operaciones de Información* (Madrid: Editorial Fragua, 2018), 172.

44 Javier Jaspe, "Las operaciones de información rusas en el conflicto del este de Ucrania", *Comunicación y Hombre*, núm. 17 (2021): 153-164.

45 Maria Snegovaya, "Putin's information warfare in Ukraine. Soviet Origins of Russia's Hybrid Warfare", *www.understandingwar.org*, 2015.

46 Tom Kington, "Vatican offers 'time off purgatory' to followers of Pope Francis tweets", *www.theguardian.com*, julio 16 de 2013.

47 Jorge Linares, "Redes criminales transnacionales: principal amenaza para la seguridad internacional en la posguerra fría", *Revista Criminalidad* 50, núm. 1 (2008): 371-384.

Es innegable que los medios de comunicación han sido controlados de tal forma que poseen un tipo de poder que los lleva a constituirse como el cuarto poder público. Forjando una relación dinámica en la interacción entre los gobernantes y los ciudadanos[48], que se explica en la actuación de los políticos contemporáneos que priorizan el pensamiento del público para llegar a ocupar un cargo de elección popular, los políticos encuentran en los medios de comunicación, dotados de perfiles ideológicos y de consumo, un aliado para lograr la vinculación de los ciudadanos con su causa. Desde la perspectiva de Monedero, en esto consiste la creación de una realidad a través del control de los medios de comunicación que, en medio de la sociedad de la información, genera una posición de ventaja para llegar al poder[49].

La posibilidad de presentar una noticia difundiendo determinada información sobre acontecimientos a los que el público no tiene acceso directo puede incidir en la deliberación democrática. Así las cosas, los medios de comunicación de masas eligen los hechos que quieren comunicar de acuerdo con sus agendas mediáticas, con lo cual se evidencia que son actores políticos en medio de un escenario basado en relaciones de poder y que actúan conforme a sus intereses[50]. Por eso, Walter Lippman sostuvo que el pensamiento humano mezcla el "pseudoambiente" que presentan los medios de comunicación con la realidad, modificando su comportamiento y actuando de tal forma que perjudican el contexto real[51]. Esta idea es respaldada por Noam Chomsky[52], que habla de la alteración en el ejercicio de la democracia, donde el público acepta algo que inicialmente no desea bajo la influencia de la propaganda, lo que explica diciendo que solo algunos intelectuales entienden los intereses comunes, lo que le conviene a la sociedad, pero la gente común no percibe estas cosas[53].

José Antolín manifiesta que, en organizaciones como la OTAN y la OEA, la comunicación estratégica (STRATCOM) es fundamental para mantener las relaciones internacionales. Por eso, desde la labor del Director de Comunicación (COMDIR),

48 Gonzalo Farrera, "Los medios de comunicación frente al poder del Estado", *Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM*, 2012.

49 Juan Carlos Monedero, *El gobierno de las palabras: política para tiempos de confusión*, 2ª. ed. (Madrid, Fondo de Cultura Económica de España, 2011), 174.

50 Bernadette Califano, "Los medios de comunicación, las noticias y su influencia sobre el sistema político", *Revista Mexicana de Opinión Pública*, núm.19 (2015): 61-78.

51 Walter Lippman, *Public Opinion* (New York: Free Press, 1997), 288.

52 Noam Chomsky, *El Control de los Medios de Comunicación* (Buenos Aires: Libros Tauro, 2003), 32.

53 Chomsky, *El Control*, 32.

se aplican de manera coordinada las capacidades y herramientas comunicativas en la diplomacia, información pública y pública militar, como operaciones de información y psicológicas para alcanzar el fin último[54].

No obstante, existen las *fake news*, que reemplazan los medios y métodos conocidos en el *hard power*. Por eso, David Alandete afirma que se emplean noticias falsas y otras narrativas alternativas para socavar la estabilidad de la democracia, pero que también inciden sobre la población nacional[55]. Un ejemplo de ello es la creación de una red de *bots* (Kelihos) que mediante correos maliciosos bloquean la información personal de las víctimas para posteriormente pedir un rescate económico para su recuperación.

La manipulación de la información es notoria en Colombia en dos casos. El primero sucede en diciembre del año 2021, cuando comunidades del sur del Chocó denuncian que existen operativos desarrollados por dudosos militares en caseríos donde afirman que los militares se presentaban como guerrilleros y atacaban a la población civil, engañándolos con su aspecto en medio de operaciones dirigidas a la captura de alias 'Schumager', un mando intermedio del Ejército de Liberación Nacional (ELN) [56].

El segundo caso sucede en marzo del año 2022, en la vereda el Remanso de Puerto Leguizamo, Putumayo, donde la información suministrada indica que, de las once personas muertas que se fueron presentadas como disidentes del frente 48, siete de los muertos eran civiles, lo que lleva a que el excomandante de las Fuerzas Militares (FFMM) presente un informe y a que el exministro Molano sea llamado a moción de censura en sesiones del Congreso[57]. Los dos casos se suman a otros que exponen situaciones en las que se manipula la información para favorecer los querencias de uno de los involucrados.

[54] José Luis Antolín García, "La comunicación estratégica (STRATCOM) en las organizaciones internacionales", en *Documentos de Seguridad y Defensa 72. La comunicación estratégica*, ed. Ministerio de Defensa, España (Instituto Español de Estudios Estratégicos, 2017).

[55] David Alandete, *Fake News: La nueva arma de destrucción masiva* (Barcelona: Editorial Planeta, 2019), 29.

[56] Camilo Álzate, "Las denuncias sobre dudosos operativos militares en el río San Juan en Chocó", *Elespectador.com*, Conflicto, 12 diciembre de 2021, en línea.

[57] Cristina Navarro, "Procuraduría pide informe a Fuerzas Militares por operación en Putumayo", *Caracol Radio,* Justicia, 31 de marzo de 2022.

Enfrentando el desafío

Para abordar los desafíos de la guerra de la información, se encuentra como una opción la formación de los ciudadanos en temas mediáticos, proporcionando bases con las que sean capaces de crear un pensamiento crítico frente a lo que ven. Además, se necesita que los gobiernos actúen activamente en temas como la regulación de las plataformas digitales y estrategias efectivas de verificación de información para impedir la propagación de la información falsa a través de las noticias y otros medios.

La manipulación y la desinformación son desafíos para atender, por la influencia que ejercen en la imagen de las instituciones y en la dinámica social. Por eso, enfrentar el desafío demuestra la necesidad de planear una estrategia con un enfoque multidimensional que involucre a la sociedad en el trabajo realizado por la seguridad humana.

Asimismo, el empleo de tácticas sofisticadas para distorsionar hechos y crear narrativas engañosas promueve ideologías que generan confusión, alimentan la polarización y debilitan la estabilidad social y política. También, es imprescindible crear estrategias enfocadas en evitar que la información predisponga la toma de decisiones que puedan afectar la buena calidad de vida y la seguridad de las personas por causa de los ataques cibernéticos para obtener información personal y utilizarla con malas intenciones. Por eso, es importante contar con planes y programas que siguen los movimientos que en la red afectan la seguridad cibernética y a través de los que se fortalecen las conocidas *fake news* y los mensajes que impulsan movimientos que atentan contra la seguridad y el orden público. Igualmente, la batalla se fundamenta en el trabajo coordinado y complementado con una respuesta integral y colaborativa entre el Estado, las organizaciones y los ciudadanos.

La militarización del espacio exterior

Vincular al espacio como un nuevo escenario de operaciones es una perspectiva que deja ver una realidad en la que, desde 1966, países como Estados Unidos han contemplado la posibilidad de llevar las confrontaciones hasta ese punto, atentando contra la infraestructura espacial de sus adversarios desde bases terrestres y aéreas. Este ejemplo fue seguido por la Unión Soviética un año más tarde, cuando investigó

sobre el impacto que tendría disparar armas desde tierra o desde el espacio[58]. Lo anterior es una demostración de la consideración del espacio como un lugar en donde es pertinente militarizar las actividades y en donde se desarrollan capacidades diferentes por medio de satélites y otras herramientas que hacen parte de las operaciones militares contemporáneas, lo que se transforma en una preocupación en el escenario internacional[59].

Aunque el Consejo de Seguridad de la ONU prohibió que esto sucediera, ya que el espacio es una zona de investigación y exploración, paradójicamente el Derecho Internacional, en 1967, estableció medidas insuficientes para lo que se debe enfrentar en la guerra contemporánea, lo que deja ver que es importante contar con normas que proporcionen fundamentos jurídicos y políticos para el uso de armamentos en este nuevo dominio de la guerra[60].

Para 1979, las diferencias entre Estados Unidos y la URSS llevaron a los Acuerdos SALT-II, en donde se prohibía el despliegue de satélites que no llegan a orbitar alrededor del planeta. Sin embargo, estos no entraron en vigencia porque el Senado de Estados Unidos no lo ratificó y, por el contrario, se reforzó el poder militar de Norteamérica, incluso en la fabricación de armas antisatélite[61]. José Manuel Ramírez ya preveía este desafío en el espacio exterior. Por eso, indicó que las implicaciones de esta militarización están en la competencia por el control y acceso a los activos espaciales, la destrucción de satélites y la interrupción de servicios vitales, lo que termina causando preocupaciones éticas y humanitarias relacionadas con el desarrollo de armas autónomas y sistemas de inteligencia artificial en el espacio[62].

Asimismo, el papel que los satélites desempeñan en la comunicación, la navegación y la recopilación de información los convierte en objetivos potenciales en caso de conflictos[63]. Por eso, pueden ser destruidos con armas antisatélite o mediante interferencia electrónica, lo que lleva la inseguridad hasta un nuevo dominio. La dependencia de las comunicaciones satelitales y la navegación por GPS se extiende a numerosos sectores, incluyendo el transporte, las comunicaciones, la banca y

58 Bhupendra Jasani, *Espacio exterior: ¿campo de batalla del futuro?* (Estocolmo: Editorial Taylor y Francis, 1978), 163-174.

59 Cesáreo Gutiérrez, "La militarización del espacio ultraterrestre", *Revista Electrónica de Estudios Internacionales*, núm. 12 (2006): 1-30.

60 F. Lay, "Usi pacifici dello spazio extra-atmosferico", *La Comunità Internazionale*, núm.2 (1979): 383-398.

61 Lay, "Usi pacifici dello spazio".

62 José Manuel Ramírez, "La militarización del espacio exterior y la vocación estelar de la carrera de armamentos", *Boletín de Información*, núm. 186 (1985): 84.

63 Jordán, "Competición entre grandes potencias".

la asistencia humanitaria. La destrucción de satélites o la interferencia con sus funciones esenciales puede generar caos, pérdida de vidas y daños económicos, así como afectar la capacidad de respuesta en situaciones de crisis[64]. Es notable que la falta de supervisión y control humano en el uso de estas armas podría tener consecuencias devastadoras. Además, existe el riesgo de una escalada armamentista en el espacio que aumentaría la posibilidad de conflictos y afectaría negativamente la seguridad global[65].

Ante este fenómeno, una posible respuesta es la cooperación internacional, con la que se establecen normas y acuerdos que regulen la militarización del espacio. Este desafío, también, debe incitar a un trabajo alejado de la corrupción cuando se trata de actividades espaciales militares y fortalecer la confianza mutua para consolidar la seguridad y la protección de las posesiones espaciales, sin poner en peligro la seguridad humana ni socavar los principios éticos fundamentales, y de los intereses de la humanidad en el espacio.

Discusión

Con el incremento de la globalización, el planeta se convirtió en espacio de una sociedad tecnológicamente avanzada, que abrió campo a nuevos dominios de la guerra para desafiar la seguridad humana. Dentro de los retos que sobresalen se enumeran la ciberguerra, la guerra de la información y la militarización del espacio, fenómenos que amenazan la infraestructura crítica, la privacidad, la estabilidad social y los derechos humanos.

Primero, los desafíos de la ciberguerra se plantean ante la posibilidad de ataques cibernéticos dirigidos a la infraestructura crítica importante, con el fin de mantener segura la vida de los seres humanos y satisfacer sus requerimientos en temas de salud, comunicación y transporte. Este ámbito, además, se complementa con problemas como el robo de información y de identidad, utilizados para sacar provecho de las víctimas u obtener algún tipo de información de interés del atacante.

Segundo, la guerra de la información se fundamenta en el control y división en la población por medio de la desinformación con la que se afecta la imagen de las

[64] Federico Aznar, "El espacio exterior, una nueva dimensión de la Seguridad", *Boletín Instituto Español de Estudios Estratégicos* (2021).

[65] Javier Jordán y Josep Baqués, "Robots, ciberguerra y militarización del espacio", *Revista Ensayos Militares* 4, núm. 2 (2018): 47-57.

instituciones y se influye sobre la opinión pública usando noticias engañosas y difíciles de verificar. Esto genera ventaja para quien posee la información real y el control sobre el pensamiento del receptor del mensaje tendencioso que se quiere emitir. Finalmente, la militarización del espacio se convierte en un riesgo significativo para la seguridad global y humana como consecuencia de la competencia por el control y acceso a los activos espaciales que pueden ser objetivos militares como parte de estrategias que incluyen el desarrollo de armas autónomas y sistemas de inteligencia artificial en el espacio.

Respuestas y medidas necesarias

Ante estos desafíos, es imperativo que la comunidad internacional y los actores relevantes tomen medidas para fortalecer la seguridad humana en los nuevos dominios de la guerra. La reciprocidad internacional, la entrega de información y la creación de acuerdos y normas son esenciales para abordar la ciberguerra, la guerra de la información y la militarización del espacio. Además, se requiere una inversión continua en tecnología y capacitación para fortalecer las defensas cibernéticas y salvaguardar la infraestructura crítica.

La ciberguerra, la guerra de la información y la militarización del espacio son los medios a tener en cuenta a la hora de plantear medidas de atención y mitigación del conflicto en nuevos dominios de la guerra que atentan contra la estabilidad social y los derechos humanos, lo que obliga a la intervención de quienes se encuentran en el poder, de las organizaciones internacionales y de las personas representadas en la sociedad para detener los avances en los nuevos escenarios de confrontación.

Conclusiones

En conclusión, los nuevos dominios de la guerra representan desafíos significativos para la seguridad humana en la era moderna que se concentran en el ciberespacio, las operaciones de información y la militarización del espacio exterior. Estos ámbitos deben ser atendidos con estrategias y normas con las que se fortalezca la seguridad ante una guerra híbrida que involucra al ciberespacio y la infraestructura digital.

Lo mismo sucede con las guerras de información, en donde la ventaja la tiene quien posee la información y victimiza a quien es víctima de un mensaje errado que se transmite con la manipulación informativa. Por eso, es preciso crear un ambiente en donde el reconocimiento de la información falsa y la capacidad de crear juicios

propios con base en la información real recibida sean la medida para detener la desinformación que genera conflictos en los nuevos dominios.

En referencia a la militarización del espacio exterior, se determina este fenómeno como un desafío, por cuanto no existe una norma que regule la creciente actividad militar en el espacio, lo que impulsa la vigilancia y el desarrollo de armas antisatélite y, por ende, conlleva riesgos para la seguridad global. De ahí se expone la necesidad de estudiar los avances tecnológicos que se presentan en los dominios de guerra tradicionales y nuevos, para, de esta forma, detener cualquier efecto que ello produjera en el mundo.

En síntesis, abordar los desafíos en estos nuevos dominios de la guerra requerirá la coordinación de gobiernos, organizaciones internacionales y de las personas en el proceso de desarrollo de maniobras y políticas efectivas que promuevan la seguridad humana en nuevos escenarios de conflicto. De esta forma, es posible proteger los derechos y la seguridad de las personas en un entorno cada vez más complejo y tecnológico.

Referencias

Acevedo, Christian, Valentina Ballesteros, y María Antonieta Corcione. "Seguridad humana y seguridad multidimensional, su enfoque y utilidad para proteger los derechos humanos [en línea]". *Revista Científica General José María Córdova* 20, núm. 40 (2022): 1106. https://doi.org/10.21830/19006586.1081

Alandete, David. *Fake News: La nueva arma de destrucción masiva.* Barcelona: Editorial Planeta, 2019. https://www.marcialpons.es/media/pdf/40021_Fake_News.pdf

Alberts, David S., y Richard E. Hayes. *Power to the edge: Command... control... in the information age.* Office of the Assistant Secretary of Defense Washington DC Command and Control Research Program (CCRP). Washington, D.C.: CCRP, 2003. http://www.dodccrp.org/files/Alberts_Power.pdf

Álzate, Camilo. "Las denuncias sobre dudosos operativos militares en el río San Juan en Chocó". *Elespectador.com*, Conflicto, 12 diciembre de 2021, en línea. https://www.elespectador.com/colombia-20/conflicto/denuncias-sobre-operativos-militares-irregulares-en-el-rio-san-juan-choco/

Antolín García, José Luis. "La comunicación estratégica (STRATCOM) en las organizaciones internacionales". en *Documentos de Seguridad y Defensa 72. La comunicación estratégica*, ed. Ministerio de Defensa, España. Instituto Español de Estudios Estratégicos, 2017. https://dialnet.unirioja.es/servlet/articulo?codigo=6696731

Arquilla, John y David Ronfeldt. "Cyberwar is coming!". En *In Athena's Camp: Preparing for Conflict in the Information Age*, editado por John Arquilla y David Ronfeldt, 23-60. Santa Monica, CA: RAND Corporation, 1997. https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

Aznar, Federico. "El espacio exterior, una nueva dimensión de la Seguridad". *Boletín Instituto Español de Estudios Estratégicos* (2021). https://www.ieee.es/Galerias/fichero/docs_analisis/2021/DIEEEA10_2021_FEDAZN_EspacioExterior.pdf

Barbas, Ángel. "Educomunicación; desarrollo, enfoques y desafíos en un mundo interconectado". *Foro de Educación*, núm. 14 (2012): 157-175. https://dialnet.unirioja.es/servlet/articulo?codigo=4184243

Bauluz, Alfonso. *Prensa y manipulación. El Pentágono y las Operaciones de Información.* Madrid: Editorial Fragua, 2018.

Beuchot, Mauricio. *Hechos e interpretaciones: Hacia una hermenéutica analógica*. México D.F.: Fondo de Cultura Económica, 2016. https://doi.org/10.24310/Contrastescontrastes.v0i0.1510

Becerra Ortiz, Jairo, Bibiana Beatriz Luz Clara, John Grover Dorado, John Velandia, Jose Araoz Fleming y Marco Emilio Sánchez Acevedo. "Implicaciones jurídicas en el entorno del *big data*: el caso del app Navega Seguro". *Novum Jus* 17, núm. 1 (2023): 357-388. https://doi.org/10.14718/NovumJus.2023.17.1.15

Bisky, Lothar. *Crítica de la Teoría Burguesa de la Comunicación de Masas*. Madrid: Ediciones de la Torre, 1982.

Bowers, L. "Safewards: un nuevo modelo de conflicto y contención en salas psiquiátricas". *Revista de enfermería psiquiátrica y de salud mental* 21, núm. 6 (2014): 499-508. https://doi.org/10.1111/jpm.12129

Califano, Bernadette. "Los medios de comunicación, las noticias y su influencia sobre el sistema político". *Revista Mexicana de Opinión Pública*, núm.19 (2015): 61-78. https://doi.org/10.1016/j.rmop.2015.02.001

Carvajal, Jorge. "Seguridad Humana, en el contexto de la lucha contra el terrorismo". *Novum Jus* 2, núm. 1 (2008): 205-234. https://novumjus.ucatolica.edu.co/article/view/896/923

Chomsky, Noam. *El Control de los Medios de Comunicación.* Buenos Aires: Libros Tauro, 2003. https://www.solidaridadobrera.org/ateneo_nacho/libros/Noam%20Chomsky%20-%20El%20control%20de%20los%20medios%20de%20comunicacion.pdf

Clarke, Richard A. y Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* Madrid: Ecco, 2011.

David, Charles-Phillippe y Raúl Quiroz, editores. *La Guerra y la Paz: Enfoque Contemporáneo Sobre la Seguridad y la Estrategia*. Barcelona: ICARIA, 2008.

De Esteban, Jorge. "Los medios de comunicación como control de poder político". *Revista de Derecho Político*, núm. 42 (1997): 11-34. https://doi.org/10.5944/rdp.42.1996.8694

Diniz, Eduardo. "Tecnologías de back-office: desafíos no mundo interconectado". en *Administração Bancária: uma visão aplicada*, 177-200. Rio de Janeiro: Editora FGV, 2014. https://www.researchgate.net/publication/304039180_Tecnologias_de_back-office_desafios_no_mundo_interconectado

Farrera, Gonzalo. "Los medios de comunicación frente al poder del Estado". *Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM*, 2012. https://archivos.juridicas.unam.mx/www/bjv/libros/6/2967/12.pdf

García, Elena. "Altas tecnologías, conflictos armados y seguridad humana". *Araucaria* 18, núm. 36 (2016): 265-293. https://doi.org/10.12795/araucaria.2016.i36.13

Gutiérrez, Cesáreo. "La militarización del espacio ultraterrestre". *Revista Electrónica de Estudios Internacionales*, núm. 12 (2006): 1-30 http://www.reei.org/index.php/revista/num12/articulos/militarizacion-espacio-ultraterrestre

Hernández, Rafael Grasa. "Vínculos entre seguridad, paz y desarrollo: evolución de la seguridad humana: de la teoría al programa político y la operacionalización". *Revista CIDOB d'Afers Internacionals*, núm. 76 (2006): 9-46. http://www.jstor.org/stable/40586270

Ilivitzky, Matias. "Debates actuales sobre el orden liberal internacional". *Comillas Journal of International Relations*, núm. 24 (2022): 35-51. https://doi.org/10.14422/cir.i24.y2022.003

Jasani, Bhupendra. *Espacio exterior: ¿campo de batalla del futuro?* Estocolmo: Editorial Taylor y Francis, 1978.

Jaspe, Javier. "Las operaciones de información rusas en el conflicto del este de Ucrania". *Comunicación y Hombre*, núm. 17 (2021): 153-164. https://doi.org/10.32466/eufv-cyh.2021.17.623.153-164

Jordán, Javier. "Competición entre grandes potencias y militarización del espacio exterior". *Araucaria*, núm. 53 (mayo 2023): 169-194. https://doi.org/10.12795/araucaria.2023.i53.07

Jordán, Javier y Josep Baqués. "Robots, ciberguerra y militarización del espacio". *Revista Ensayos Militares* 4, núm. 2 (2018): 47-57. https://revistaensayosmilitares.cl/index.php/acague/article/view/57

Kington, Tom. "Vatican offers 'time off purgatory' to followers of Pope Francis tweets". *www.theguardian.com*, julio 16 de 2013. https://www.theguardian.com/world/2013/jul/16/vatican-indulgences-pope-francis-tweets

Krause, Keith. "Seguridad humana: ¿ha alcanzado su momento?". *Papeles de cuestiones internacionales*, núm. 90 (2005): 19-29

https://www.fuhem.es/media/ecosocial/file/Cohesi%C3%B3n%20Social/Desigualdad,%20pobreza%20y%20exclusi%C3%B3n/Seguridad_humana_ha_llegado_su_momento_KKrause.pdf

Lay, F. "Usi pacifici dello spazio extra-atmosferico". *La Comunità Internazionale*, núm.2 (1979): 383-398.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monidca: RAND Corporation, 2009. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Linares, Jorge. "Redes criminales transnacionales: principal amenaza para la seguridad internacional en la posguerra fría". *Revista Criminalidad* 50, núm. 1 (2008): 371-384. http://www.scielo.org.co/pdf/crim/v50n1/v50n1a12.pdf

Lippman, Walter. *Public Opinion.* New York: Free Press, 1997.

Lynn III, William J. "A Military Strategy for the New Space Environment". *The Washington Quarterly* 34, núm. 3 (2011): 7-16. https://doi.org/10.1080/0163660X.2011.586933

Marques, Bernardo y Marcelo Quiroga. "La Cuarta Revolución Industrial y los impactos de un mundo interconectado, en la libertad, seguridad e intimidad". *Derecho y Cambio Social*, núm. 55 (2019): 238-273. https://dialnet.unirioja.es/servlet/articulo?codigo=6967898

Martín, Antonio. "Ciudadanía global. Un estudio sobre las identidades sociopolíticas en un mundo interconectado". *ARBOR Ciencia, Pensamiento y Cultura* 193, núm. 786 (2017): 14. http://dx.doi.org/10.3989/arbor.2017.786n4010

Molina Losada, Hevert. "El ciberespacio un escenario moderno para los sistemas de seguridad". Tesis de especialización en Administración de Seguridad, Universidad Militar Nueva Granada, 2017. http://hdl.handle.net/10654/17455

Monedero, Juan Carlos. *El gobierno de las palabras: política para tiempos de confusión*, 2ª. ed. Madrid: Fondo de Cultura Económica de España, 2011.

Navarro, Cristina. "Procuraduría pide informe a Fuerzas Militares por operación en Putumayo". *Caracol Radio,* Justicia, 31 de marzo de 2022. https://caracol.com.co/radio/2022/03/31/judicial/1648733540_015210.html

Pérez de Armiño, Karlos. "El concepto y el uso de la seguridad humana: análisis crítico de sus potencialidades y riesgos". *Revista CIDOB d'Afers Internacionals*, núm. 76 (2006): 59-77. http://www.jstor.org/stable/40586272

Pizarroso, Alejandro. "Aspectos de propaganda de guerra en los conflictos armados más recientes". *Redes.com*, núm. 5 (2009): 49-65. https://dialnet.unirioja.es/descarga/articulo/3673591.pdf.

Ramírez, José Manuel. "La militarización del espacio exterior y la vocación estelar de la carrera de armamentos". *Boletín de Información*, núm. 186 (1985): 84. https://dialnet.unirioja.es/servlet/articulo?codigo=4770088

Rid, Thomas. *Active measures: The secret history of disinformation and political warfare*, 1ra. Edición. New York: Farrar, Straus, and Giroux, 2020.

Rodríguez, Rafael. "¿Qué seguridad? Riesgos y amenazas de internet en la seguridad humana". *Araucaria* 18¸ núm. 36 (2016): 391-415. https://doi.org/10.12795/araucaria.2016.i36.18

Sánchez, Marco. "La inteligencia artificial en el sector público y su límite respecto de los derechos fundamentales". *Estudios Constitucionales* 20, núm 2 (2022): 257-284. https://doi.org/10.4067/S0718-52002022000200257

Sierra-Zamora, P. A. y A. Castaño-Bedoya. "Guerras híbridas, irrestrictas, asimétricas y jurídicas en el nuevo orden mundial". *Revista Científica General José María Córdova* 20, núm. 40 (2022): 852-869. https://doi.org/10.21830/19006586.1058

Singer, P.W. y Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.

Snegovaya, Maria. "Putin's information warfare in Ukraine. Soviet Origins of Russia's Hybrid Warfare". *www.understandingwar.org*, 2015. https://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf

Stein, George. "La Guerra de Información". *Air & Space Power Journal*, en línea (1996). http://www.airpower.maxwell.af.mil/apjinternational/apj-s/1996/2trimes96/stein.html

Torres Soriano, Manuel. "Operaciones de influencia vs. desinformación: diferencias y puntos de conexión". *Documento de Opinión IEEE*, núm. 64 (2022): 16. https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO64_2022_MANTOR_Operaciones.pdf

Torrijos, Vicente y Daniel Jiménez. "Tendencias en el estudio de la seguridad en un quinto dominio de la guerra". *Cuadernos de la Guardia Civil. Revista de Seguridad Pública*, núm. 65 (2021): 73-92. https://biblioteca.guardiacivil.es/cgi-bin/koha/opac-retrieve-file.pl?id=bf9af1dc96ece946894cc4a42bb4f676

Ulloa Plaza, Jorge y María Angélica Benavides Casals. "Moralidad, guerra y derecho internacional. Tres cuerdas para un mismo trompo: la humanidad". *Novum Jus* 17, núm. 1 (2023): 259-282. https://doi.org/10.14718/NovumJus.2023.17.1.11