RELIGACIÓN
REVISTA

La ciberguerra: una aproximación conceptual

Cyberwarfare: a conceptual approach

Yamil Fernando Garcia Latorre, Yonnathan Jose Torres Gomez

Resumen

El objetivo general de esta investigación fue analizar algunas proposiciones teóricas sobre la ciberguerra y sus efectos en la dinámica venezolana. Se apoyó en el enfoque cuantitativo de tipo documental. Entre las conclusiones, resaltan que esta forma de ataque está dirigida a disminuir la capacidad del Estado – Nación que surgió con el tratado de Westfalia, en el cual nace el principio de soberanía sustentado en tres elementos que componen este principio; gobierno, población y territorio, generando situaciones de ingobernabilidad. el entorno de la información que se encuentra alojada en el ciberespacio es un dominio global que se caracteriza por estar conformado por redes independientes en las cuales es esencial la interoperatividad. Adicionalmente, la ciberguerra responde a las nuevas tendencias geopolíticas mundiales, en las cuales existe el interés, de la destrucción de la entidad del Estado-Nación como espacio para la soberanía nacional.

Palabras claves: Estado, guerra, ciberespacio, nación.

Yamil Fernando Garcia Latorre
Universidad Militar Bolivariana de Venezuela | Caracas | Venezuela | garcialatorre95@gmail.com
http://orcid.org/0009-0003-4940-1550
Yonnathan Jose Torres Gomez
Universidad Central De Venezuela | Caracas | Venezuela | yonnathantorres@gmail.com
http://orcid.org/0009-0003-3946-7150

http://doi.org/10.46652/rgn.v9i42.1273
ISSN 2477-9083
Vol. 9 No. 42 octubre-diciembre, 2024, e2401273
Quito, Ecuador

Enviado: junio 03, 2024
Aceptado: agosto 12, 2024
Publicado: agosto 24, 2024
Publicación Continua

RELIGACIÓN CICSHAL
Centro de Investigaciones en Ciencias Sociales y Humanidades desde América Latina

Abstract

The general objective of this research was to analyze some theoretical propositions about cyberwar and its effects on Venezuelan dynamics. It was based on the documentary-type quantitative approach. Among the conclusions, they highlight that this form of attack is aimed at reducing the capacity of the State–Nation that emerged with the Treaty of Westphalia, in which the principle of sovereignty is born based on three elements that make up this principle: government, population and territory, generating ungovernable situations. The information environment that is hosted in cyberspace is a global domain that is characterized by independent networks in which interoperability is essential. Additionally, cyberwar responds to new global geopolitical trends, in which there is interest in the destruction of the entity of the Nation-State as a space for national sovereignty.

Keywords: State, war, cyberspace, nation.

Introducción

El conflicto como se observa, es inherente a la naturaleza humana y a la confrontación de intereses entre las naciones. Por lo cual, la guerra sobrevive y no tiende a desparecer, solo ha mutado, combinando entre nuevos actores y amenazas, como lo son: los problemas étnicos, religiosos, las enfermedades, la pobreza, la globalización, los desastres naturales, el narcotráfico, el terrorismo y el crimen organizado.

Autores como Neiberg (2015), afirman, que la guerra ha estado presente a lo largo de la historia de la humanidad caracterizada por tres elementos fundamentales las tecnologías militares, la organización militar y los motivos que han impulsado al desarrollo de los conflictos bélicos, los cuales clasifica en cinco periodos históricos, este fenómeno social; el primero denominado Clásico que se desarrolla durante las guerras de Grecia y Roma. El segundo Edad Media desde el año 500 DC hasta la conquista turca de Bizancio en 1453. El tercero la Era de la Pólvora 1453 – 1776 Revoluciones americanas y francesas. El cuarto "Largo siglo XIX" (de 1776 a 1918) y el quinto Contemporáneo Segunda Guerra Mundial, la Guerra Fría, hasta la actualidad.

Es significativo señalar que la guerra como fenómeno social históricamente tuvo como característica principal la monopolización del Estado, de manera que, el conflicto armado fue dirigido por el Estado-nación, pero también restringido por él (Vom Hagen, 2022). Para Warf (2015), esta nueva forma de guerra tiene como característica principal la no declaración de guerra por parte de un Estado; aun y cuando coloca en riesgo la gobernabilidad de los Estados. Por su parte Balaguer (2021), en esta misma línea argumentativa sostiene que es evidente la permeabilidad del Estado a los agentes globales que actúan en el plano financiero y comunicativo, ha determinado las dos grandes crisis del constitucionalismo frente a la globalización en este siglo XXI, en las cuales se observan la imposición de condiciones económicas que limitan la capacidad de acción del Estado.

En el ámbito militar durante el siglo XXI la característica esencial es el entorno cambiante de la guerra entre otros factores por la influencia de la globalización; especialmente por los avances de los sistemas de la información que facilitaron la aparición de un nuevo escenario que supera la guerra aeroespacial mar, tierra y aire, el cual transciende la esfera puramente militar.

Al respecto Kovacich y Jones (2016), plantean que el nacimiento del internet conllevó a nuevas formas de armas como hackers, crackers, hreakers, hacktivists, script kiddies, espionaje de la red, ataques de virus y diversas formas de malware, virus como gusanos, troyanos, caballos, errores de software, fallas de hardware, denegación de servicio entre otros.

La ciberguerra es un fenómeno verdaderamente global que representa un riesgo complejo que transciende las amenazas tradicionales, la geografía física y los preceptos tradicionales de la geopolítica a niveles macro y micro, a la vez contienen el potencial de desestabilizar una economía, ya que el atacante recopila datos que pueden monetizarse como inteligencia, que junto con otras actividades delictivas, acumula financiación para seguir ampliando la complejidad y potencia de sus tecnologías, frente a la cuales la tradicional respuesta militar terrestre a está obsoleta (Cremer et al., 2024).

De manera que, las funciones de ciberseguridad son comunes tanto a las organizaciones tanto públicas como privadas que se enfrentan a las amenazas cambiantes y generalizadas de violaciones de datos y otros eventos de seguridad peligrosos, las cuales están impregnadas de características hobbesianas entre ellas se incluyen la normalización de controles como la vigilancia a las operaciones del ciberespacio (Da Silva, 2023).

Para Quintana (2016), el siglo XX fue el escenario del desarrollo de diferente tipos de armas de destrucción masiva: atómicas, biológicas y químicas (ABC), sin embargo el siglo XXI incorporó una nueva letra la D de Digital, el cual constituye la mayor preocupación para los gobiernos para garantizar la seguridad ante la intromisión de los sistema digitales; ya que es ataque de estas características es similar a un disparo al hipotálamo. El dominio del conflicto en la ciberguerra es diferente a los conflictos tradicionales, las operaciones se realizan en un espacio virtual, las armas son también diferentes a la del combate tradicional, ya que los actores pueden utilizar técnicas para afectar la funcionalidad de los sistemas, el acceso a la información o la infraestructura. (Gudaitis et al., 2017).

Los riesgos cibernéticos, en particular los asociados con la guerra cibernética, también tienen el potencial de afectar la seguridad y causar pérdidas económicas significativas debido a su inherente imprevisibilidad y sus consecuencias de largo alcance (Cremer et al., 2024). En la era digital contemporánea, el panorama global se enfrenta un aumento generalizado de actividades en línea que trascienden las fronteras geográficas, impactando a individuos, organizaciones y Estados-Nación. La creciente adopción de la digitalización ha dado lugar a un aumento notable en el fraude cibernético, en el amplio ámbito del ciberespacio, se desarrollan numerosas actividades ilícitas, que incluye ciberataques audaces (Sarkar & Shukla, 2024).

Ahora bien, estos riesgos que constituyen un elemento central para cualquier gobierno de los cuales la República Bolivariana de Venezuela no es ajena a la realidad cambiante de la guerra, en las últimas dos décadas ha sido víctima de estos ataques que se originan entre otras razones, por la importancia geopolítica de las reservas energéticas de la República Bolivariana de Venezuela, que constituyen las principales a nivel mundial que ha experimentado ataques sin la declaración de

guerra por parte de un Estado. Sin embargo, no existe una definición clara sobre la concepción de ciberguerra en la doctrina venezolana; de manera que, el propósito de esta investigación es analizar algunas proposiciones teóricas sobre la ciberguerra y sus efectos en la dinámica venezolana.

Método

La investigación se enmarca en el enfoque cuantitativo, Hernández, Fernández, y Baptista (2016), señala que este tipo de investigación permite la generalización de los resultados que pueden ser replicados en contextos similares, a partir de la recopilación de los elementos propuestos por diversos autores. El tipo de investigación es documental Arias (2012) plantea que permite en el desarrollo amplio y profundo de un tema específico, que es la ciberguerra.

Para ello, empleará como técnica el fichaje y como instrumento la ficha, Pallela y Martins (2016), representan una guía para la sistematización de información de fuentes documentales que se encuentran en los repositorios electrónicos como en los centros de documentación con el propósito de realizar un análisis bibliométrico de las principales revistas en seguridad de Estado en las cuales se analizó el número de publicaciones durante los años 2022 y 2023 permitieron establecer la concepción del tema de ciberguerra, tanto en el contexto nacional como latinoamericano.

Resultados

La ciberguerra desde la concepcion latinoamericana

Del análisis bibliométrico efectuado a las distintas publicaciones Latinoaméricas indexadas en google académico se obtuvo como resultado que durante el periodo 2023-2024 existen aproximadamente 386 publicaciones sobre ciberguerra, cuyas principales tendencias temáticas es la seguridad de Estado, pensamiento estratégico y ciberdefensa.

Por otra parte, tanto los artículos arbitrados como los trabajos de grado son publicados en revistas e instituciones educativas vinculadas a los órganos de seguridad de Estado; de manera similar, la ciberguerra en Latinoamérica es un tema preponderantemente de interés para el ámbito militar; aun cuando tienen incidencia en diversos ámbitos como la economía, jurídico, tecnológico, ya que las ciberarmas pueden tener consecuencias semejantes con las armas tradicionales (Reale, 2023). No es casuístico, que los países con mayor número de publicaciones sobre el tema de la ciberguerra son México, Colombia, Brasil, Argentina y Venezuela ya que son los Estados con los principales ejércitos en la región Latinoamericana. Sin embargo, cada Estado tiene una definición y trata el tema de la ciberguerra según sus intereses y dispositivos tecnológicos a su disposición.

En Argentina existen un importante número de autores preocupados por el tema de ciberguerra, entre estos Reale (2023), quien sostiene que la ciberguerra genera incertidumbre en el diseño y ejecución de las tácticas para abordarla, por lo que es necesario la inteligencia estratégica militar. Asimismo, la asimetría genera que el potencial armamentístico tradicional de una nación

no necesariamente sea proporcional al poder cibernético, por lo cual un país puede tener poco armamento bélico físico pero grandes capacidades cibernéticas, o viceversa.

Para Suárez-Álvarez et al. (2023), los nuevos hábitos de consumo y los nuevos servicios generados por los avances las TIC como la digitalización, interiorizados en la cotidianeidad de la sociedad, también conllevan que los actos de ciberguerra crezcan aceleradamente como ataque a las infraestructuras civiles, el uso de códigos maliciosos como verdaderos. La digitalización permite optimizar los recursos disponibles en las vías de las telecomunicaciones. Aunado a la, interoperabilidad es un elemento esencial para para la ciberdefensa es la habilidad de sistemas, unidades o fuerzas para entregar o recibir servicios de otros sistemas, unidades o fuerzas, y usar estos servicios compartidos para permitirles operar conjuntamente en forma eficiente.

De manera que, es importante comprender el funcionamiento de la ciberguerra el autor Mexicano Lima (2023) señala que esta, se desarrolla en el ciberespacio el cual es un dominio global dentro del entorno de la información que consiste en las redes independientes de la infraestructura de la tecnología y los datos residentes, lo que contempla el internet como redes de telecomunicaciones, sistemas informáticos y procesadores u controladores integrados. Los ataques de las operaciones cibernéticas generan el mismo nivel de violencia que se produce en un conflicto armado. Por otra parte, los actores no son Estatales como las acciones tradiciones de un Estado–Nación, aunque en ocasiones estén motivadas por estos.

Por su parte Cáceres (2023), señala que ataques contra los sistemas de información tanto del sector público como el privado pueden derivar en un conflicto militar de gran escala; por ende, es imprescindible fortalecer la seguridad de la información; ya que se estima que cada año la pérdida total por delitos informáticos es mucho mayor de lo que se cree. El control del ciberespacio es fundamental en los resultados de las operaciones militares, sin embargo requieren integrarse a los dominios tradicionales para disponer de la libertad de acción y dificultar el acceso a personas no autorizadas (Ramírez, 2024).

Desde la perspectiva de defensa y seguridad el ciberespacio se clasifica como dominio operativo reconocido por la Organización del Tratado del Atlántico Norte (OTAN), junto con el tierra, mar, aire, es un elemento que ha sido ampliamente discutido en varios alcances, Brasil mencionó que incorporó por primera vez el ciberespacio como un elemento susceptible del ejercicio de la soberanía en un espacio virtual, compuesto de dispositivos informáticos conectados o no, a redes, donde la información digital de tránsito, son procesados y/o almacenados. Mientras que el ciberataque es ampliamente debatido, es concebido como las acciones (ofensivas o defensivas) realizadas contra un actor en el ciberespacio (Zaniboni, 2023)

La ciberguerra desde la concepcion venezolana

Entre los autores venezolanos preocupados por el estudio de la ciberguerra o esta nueva forma de guerra no convencional destacan Padrino y Angiolillo Fernández. Para Padrino (2023),

la principal diferencia con la guerra aeroterrestre es el desarrollo tecnológico, entre las acciones que se realizan en esta forma de guerra es el empleo de internet, la contratación de mercenarios, que se aplicado en la región de América Latina a través de la combinación de diferentes aspectos para buscar el caos y la ingobernabilidad a través del golpe suave, uso de ataques a través del internet, el empleo de las redes sociales, el paramilitarismo, el empleo del narcotráfico, la guerra ambiental, con el propósito de generar una situación de ingobernabilidad, un Estado fallido, ingobernable.

De manera que, el país ha experimentado ofensivas en el campo de la TIC´S para exploración y determinación de vulnerabilidades del país, para lograr la superioridad en el ámbito del ciberespacio y espacio electromagnético, implementando operaciones de información para afectar la percepción de la realidad para condicionar el imaginario colectivo y reducir la voluntad de lucha de la población.

Señala Padrino (2023) en la actualidad existe un teatro de operaciones virtuales con el propósito de generar una guerra multidimensional, multiforme de carácter no convencional, no lineal y no secuencial que se puede identificar como una guerra difusa, término que describe la esa cualidad que le permite existir con enormes dificultades para poder ser identificada y precisada, en ella se entrecruzan diferentes tipos y doctrinas de guerra no armada que coexisten y se entrelazan de manera rizomática y simultánea.

Existen al menos nueve tipos de guerra la psicológica, informática, tecnológica, económica, financiera, legal, informativa, logística y comunicacional y no menos de once doctrinas. De manera que, es necesario comprender el carácter multidimensional del modelo planteado con el espacio o ámbito donde se desarrollan diferentes acciones que inciden en el Estado, este representado por el espectro del conflicto a la escalada de escenarios múltiples y su incidencia es potenciada y progresiva.

Por su parte Angiolillo (2021), sostiene que se trata de una guerra de amplio espectro, una guerra difusa que tratan de la combinación y aplicación de más 12 teorías de lucha no armada que atacan el concepto de Estado – Nación que surge con el tratado de Westfalia, en el cual nace el principio de soberanía sustentado en tres elementos que componen este principio gobierno, población y territorio, estos tres elementos son amenazados en especial el centro de gravedad constituido por el gobierno nacional generando situaciones de ingobernabilidad, lo que trae aparejado la necesidad de repensar las estrategias de ejercer la soberanía y adaptase a este nuevo entorno dinámico del ciberespacio.

Conclusiones

En la bibliografía consultada coincide que las características de la ciberguerra es precisamente la no declaración de guerra por parte de un Estado; aun y cuando coloca en riesgo la gobernabilidad de los Estados, que trascienden las fronteras geográficas, impactando a individuos, organizaciones y Estados-nación, frente a la cual las formas tradicionales de la guerra aeroespacial

mar, tierra y aire están obsoletas de manera que coloca en riesgo tanto a las instituciones del sector público como a las privadas, de los cuales algunos ataques constituyen la mayor preocupación para los gobiernos para garantizar la seguridad ante la intromisión de los sistema digitales donde los actores pueden utilizar técnicas para afectar la funcionalidad de los sistemas de información.

Referencias

Angiolillo F, P. (2021). *Guerra Difusa. Congreso Dirección Estratégica IESOFANB.* UMBV.

Arias, F. (2012). *El proyecto de investigación. Introducción a la metodología* (5ta ed.). Epistema.

Balaguer, F. (2021). Las dos grandes crisis del constitucionalismo frente a la globalización en el siglo XXI. *Revista REDCE, 1*(30).

Cáceres, J. (2023). Ciberguerra,la nueva amenaza mundial del siglo XXI. Colombia y el reto de la cultura de información. *Revista de la Fuerzas Armadas, 2*(226), 46-60. https://doi.org/10.25062/0120-0631.1038

Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Ryan, B., & Materne, S. (2024). On the insurability of cyber warfare: An investigation into the German cyber insurance market. *Computers & Security*, 200-230. doi:https://doi.org/10.1016/j.cose.2024.103886

Da Silva, J. (2023). Cyber security and the Leviathan. *Computers & Security, 111*(12). https://doi.org/10.1016/j.cose.2022.102674

Gudaitis, T., Kilger, M., Malin, C., & Holt, T. (2017). Asymmetric Warfare and Psyops. In C. Malin, *Deception in the Digital Age: Exploiting and Defending Human Targets through Computer-Mediated Communications* (pp. 207–226). Academic Press. DOI:10.1016/B978-0-12-411630-6.00008-6

Hernández, S., Fernández, C., & Baptista, L. (2016). *Metodología de la investigacion.* McGraw-Hill/Interamericana.

Kovacich, G., & Jones, A. (2016). *Global Information Warfare The New Digital Battlefiel* (2da ed.). Auerbach Publications.

Lima, L. (2023). Derecho Internacional Aplicado a la CIberguerra:Principios Reguladores. *Seminario de Derecho Internacional* [Tesis licienciatura,]

Neiberg, M. (2015). Warfare in History. *International Encyclopedia of the Social & Behavioral Sciences*, 16367-16373. https://doi.org/10.1016/B0-08-043076-7/02756-X

Padrino, V. (2023). *Guerra Difusa. Una guerra multidimensional y multiforme de carácter no convencional aplicada a la República Bolivariana de Venezuela.* (1 era ed.). (UMBV, Ed.) Fondo Editorial Hormiguero.

Pallela, S., & Martins, F. (2016). *Metodología de la investigación cuantitativa* (3era ed.). FEDUPEL.

Quintana, Y. (2016). *Ciberguerra.* La Catarata.

Ramírez, A. (2024). Ciberdefensa como estrategia para la seguridad y soberanía digital en Paraguay. *Revista juídica de Investigación en ciencias jurídicas y sociales., 14*(1), 16-41.

Reale, J. (2023). Los desafíos de la ciberguerra y la importancia de fortalecer la inteligencia estratégica militar en la Argentina. *Revista de la Escuela Nacional de Inteligencia, 2*(2), 69-98.

Sarkar, G., & Shukla, S. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology, 4*(1), 25-45. https://doi.org/10.1016/j.jeconc.2024.100063

Suárez-Álvarez, R., Fernández-Martínez, L., & Martín-Cárdaba, M. (2023). *Vulnerabilidad digital: Desafíos y amenazas de la sociedad hiperconectada.* Dykinson

Vom Hagen, U. (2022). Warfare, Modern. *Encyclopedia of Violence, Peace, & Conflict, 2*(2), 265-274. https://doi.org/10.1016/B978-0-12-820195-4.00277-6

Warf, B. (2015). Cyberwar: A new frontier for political geography. *Political Geography, 46*(12), 89-90. https://doi.org/10.1016/j.polgeo.2014.07.010

Zaniboni, J. (2023). *Ciberguerra & Clausewitz: Análise dos Fenômenos da Ciberguerra no Irã e Ucrânia (2010–2015).* Universidade Federal Fluminense–UFF.

Autores

Yamil Fernando Garcia Latorre
Participante de la Maestría en Planificación y Conducción Operacional Militar, especialista en infantería, licenciado en ciencias y artes militares, egresado de la Academia Militar del Ejército Bolivariano.
Yonnathan Jose Torres Gomez
Participante de la Maestría en Planificación y Conducción Operacional Militar, especialista en infantería, licenciado en ciencias y artes militares, egresado de la Academia Militar del Ejército Bolivariano. Actualmente se desempeña como jefe del grupo de trabajo de operaciones del Cuartel General del Ejército Bolivariano.

Declaración

Conflicto de interés
No tenemos ningún conflicto de interés que declarar.
Financiamiento
Sin ayuda financiera de partes externas a este artículo.
Notas
El artículo es original y no ha sido publicado previamente.