El conflicto entre Rusia y Ucrania: una guerra de quinta generación

María Alejandra Santos Barón*

Resumen

En febrero de 2022, en la denominada Operación Militar Especial lanzada por Vladimir Putin se activó el conflicto entre Rusia y Ucrania. Este artículo busca analizar por qué el conflicto entre Rusia y Ucrania se puede configurar como una guerra de quinta generación. De esta manera, la investigación arrojó que dicha confrontación se puede catalogar como una guerra de quinta generación porque los enfrentamientos se han realizado en las ciudades, que son clasificadas como centros de gravedad militares, políticos y económicos. Así mismo, la confrontación, pese a realizarse en el plano tradicional de la guerra, también se ha desarrollado en su quinto dominio, el ciberespacio, y, finalmente, se identificó la participación de las compañías militares privadas de seguridad en el conflicto. Al respecto, el enfoque metodológico cualitativo permite analizar las características de las guerras de quinta generación a la luz de un estudio de caso internacional.

Palabras clave: Rusia; Ucrania; conflicto; guerra de quinta generación; ciberespacio.

THE CONFLICT BETWEEN RUSSIA AND UKRAINE: A FIFTH GENERATION WAR

Abstract

In February 2022, the so-called Special Military Operation launched by Vladimir Putin activated the conflict between Russia and Ukraine. This article seeks to answer why the conflict between Russia and Ukraine can be configured as a fifth-generation war. The research found that the confrontation between Russia and Ukraine can be categorized as a fifth-generation war because the fighting is taking place in cities, which are categorized

* Magíster en Seguridad y Defensa Nacional, Escuela Superior de Guerra "General Rafael Reyes Prieto" (Colombia); politóloga, Universidad del Rosario (Colombia). Directora de la Facultad de Ciencias Políticas y Gobierno, Universidad Pontificia Bolivariana. Miembro del grupo de investigación CIPJURIS, Universidad Pontificia Bolivariana. [mariaa.santos@upb.edu.co]; [https://orcid.org/0000-0002-3073-9741].

Recibido: 8 de febrero de 2024 / Modificado: 4 de marzo de 2024 / Aceptado: 6 de marzo de 2024

Para citar este artículo:

Santos Barón, M. A. (2024). El conflicto entre Rusia y Ucrania: una guerra de quinta generación. *Opera*, 35, 37-61.

DOI: https://doi.org/10.18601/16578651.n35.03

as the military, political and economic centers of gravity. Furthermore, the confrontation, despite taking place on the traditional plane of warfare, has also involved the fifth domain of warfare, cyberspace, and finally, the involvement of private military companies in the conflict was identified. In this respect, the qualitative methodological approach allows us to analyses the characteristics of fifth generation warfare in the light of an international case study.

Key words: Russia; Ukraine; conflict; fifth generation warfare; cyberspace.

INTRODUCCIÓN

El 24 de febrero de 2022, el gobierno de Vladimir Putin lanzó la "Operación Militar Especial" contra Ucrania. "La narrativa rusa justifica sus acciones debido al supuesto genocidio ucraniano en el Dombás y al constante avance de la OTAN sobre Moscú" (Valle, 2022). El siguiente artículo de reflexión tiene como objetivo analizar el conflicto entre Rusia y Ucrania, catalogándolo como una guerra de quinta generación, porque se presentan estas características principales: primero, la confrontación se enfoca en las ciudades, como centros de gravedad militares, políticos, económicos y sociales; segundo, el escenario de confrontación se ha ampliado a otros dominios de la guerra (ciberespacio y cognitivo); finalmente, las guerras de quinta generación involucran la participación de actores no estatales como las compañías militares de seguridad, que han adquirido un papel importante en los conflictos recientes. Para este propósito, el documento cuenta con un enfoque metodológico cualitativo:

> … la investigación bajo el enfoque cualitativo se sustenta en evidencias que se orientan más hacia la descripción profunda del fenómeno con la finalidad de comprenderlo y explicarlo a través de la aplicación de métodos y técnicas derivadas de sus concepciones y fundamentos epistémicos, como la hermenéutica, la fenomenología y el método inductivo. (Sánchez, 2019, p. 104)

La investigación es descriptiva y analítica, mediante la recolección de información de fuentes secundarias, así como su respectivo análisis documental. Para ello, se consultaron revistas especializadas en seguridad, defensa, relaciones internacionales, así como la búsqueda de fuentes periodísticas, para realizar el estudio de caso.

Se utilizó la metodología de estudio de caso, ya que permite analizar una situación compleja (aula) basada en el entendimiento de dicha situación, obtenido mediante su descripción y análisis. Esta metodología implica un entendimiento comprehensivo, una descripción extensiva y un análisis de la situación (Murillo, s. f.); asimismo, "permite investigar determinados fenómenos, desde múltiples perspectivas y no desde la influencia de una sola variable, en los que se busca dar respuesta a cómo y por qué ocurren" (Expósito, 2012, p. 87). El estudio de caso permite una exploración profunda y detallada de fenómenos complejos. Al centrarse en un caso específico, los investigadores pueden examinar en detalle las múltiples dimensiones y variables que influyen en el fenómeno estudiado.

En el contexto de un conflicto de quinta generación, donde se observa una evolución en los dominios de la guerra y la naturaleza cambiante de los actores y sus objetivos, las variables de investigación analizadas para esta investigación son: los dominios físicos (terrestre, aéreo, marítimo, espacio exterior), tecnológicos (ciberespacio) y cognitivos. También los actores (estatales, no estatales, compañías militares privadas, etc.) y la variable relacionada con la naturaleza cambiante de los actores y sus objetivos, es decir, cómo los actores interactúan en el contexto de acuerdo con sus capacidades y los objetivos estratégicos trazados. Teniendo en cuenta estas variables se analiza el conflicto entre Rusia y Ucrania, para poder afirmar que, de acuerdo con las características de las guerras de quinta generación, este conflicto se puede catalogar como tal.

Este artículo se encuentra vinculado al Grupo de Investigación en Ciencia Política y Derecho de la Universidad Pontificia Bolivariana, seccional Bucaramanga.[1]

Para este propósito, el artículo está dividido en tres partes. En primer lugar, se analizará el concepto de guerra de quinta generación; en segundo lugar, se analizará el conflicto entre Rusia y Ucrania, teniendo en cuenta el concepto de guerra de quinta generación y, en tercer lugar, se presentarán las conclusiones.

LAS GUERRAS DE QUINTA GENERACIÓN

William Lind (2005) escribió el artículo "El rostro cambiante de la guerra: hacia la Cuarta Generación", el cual explicaba la evolución que ha tenido la guerra. De esta manera, identificó cuatro generaciones de la guerra, que explicaban los cambios en la conducción de la conflagración. La primera generación, "la guerra de la táctica de líneas y columnas, en la cual las batallas eran formales y el campo de batalla era ordenado, duró aproximadamente desde 1648 hasta 1860" (p. 14). Los Ejércitos combaten en orden cerrado[2] y con una disciplina férrea que tiene el propósito de conseguir una mayor eficacia de fuego. El clásico ejemplo de esta guerra de primera generación son las batallas de Waterloo, la Guerra de Secesión, entre otras.

La guerra de segunda generación implicó un aumento en la potencia de fuego en masa, casi todo fuego de artillería indirecto. En esta generación la tecnología fue vital porque permitió incrementar el poder de fuego de los ejércitos, con armamentos como las ametralladoras. Así mismo, aparece el concepto de guerras de trincheras, que fue desarrollado en la Primera Guerra Mundial, en la cual los ejércitos combatientes mantenían líneas estáticas de fortificaciones que les permitían

[1] Este artículo también es producto de las investigaciones realizadas en el marco de la asignatura Seguridad y Conflictos Urbanos del Programa de Ciencias Políticas y Gobierno de la UPB, Bucaramanga.

[2] El "orden cerrado" en una guerra se refiere a la manera en que las tropas militares se organizan en una formación cerrada, con los soldados alineados uno al lado del otro en filas y columnas, siguiendo una estructura predefinida y en estrecha coordinación con sus compañeros de unidad. Esta táctica se utiliza para lograr una mayor eficacia de fuego y también para mantener la disciplina y la cohesión de la unidad en situaciones de combate.

mantener unas posiciones fijas en un tiempo determinado.

La guerra de tercera generación, que se desarrolló en la Segunda Guerra Mundial (1939-1945), es reconocida como la guerra relámpago (*blitzkrieg*) o guerra de maniobra (Lind, 2005). En esta guerra fueron clave los famosos tanques alemanes que permitían ganar un territorio gracias a la velocidad que proporcionan y al factor sorpresa. En esta generación se produce una mecanización de la guerra, en donde la industria militar crece rápidamente por la aparición de los tanques mecanizados, las aeronaves, los submarinos entre otros.

En las guerras de cuarta generación aparecen nuevos actores no estatales que se configuran como amenazas, en particular los grupos terroristas como Al Qaeda, Hamas, entre otros, que logran cambiar la conducción de la guerra. También aparecen otros actores no estatales como los medios de comunicación, ONG, corporaciones, entre otros, que hacen que el Estado pierda poder (Gajat, 2018). Otra particularidad de la cuarta generación es que "busca derrumbar al enemigo internamente en vez de destruirlo físicamente […] La guerra de la cuarta generación se libra en un espacio aparentemente difuso e indefinido. La distinción entre guerra y paz será borrosa" (Lind, 1989). En esta etapa, el teatro de operaciones se expande y los conflictos no se librarán solo en el plano militar. Por eso aparecen conceptos como los de guerra asimétrica y guerra híbrida, que explican cómo se libra la guerra en el siglo XXI.

Sin embargo, hoy en día –en parte, gracias a la tecnología– ha emergido una nueva generación de la guerra. El concepto de guerra de quinta generación "tuvo su origen alrededor del año 2005. Roy Alderman (2015) la califica como una guerra sin contacto y silenciosa, que está fundamentada básicamente en el aprovechamiento masivo de los medios cibernéticos y en el dominio de la mente" (Barrera *et al.*, 2021, p. 10). En esta generación aparecen nuevos actores, espacios y medios donde se desarrolla la guerra, en ese sentido se expanden los "escenarios de conflicto, para incluir el físico (tierra, aire, mar, espacio exterior), la información (cibernética) y la cognitiva y social (los dominios políticos)" (Álvarez *et al.*, 2018, p. 192).

Donald Reed creó un marco conceptual para entender la guerra de quinta generación, que consta de cuatro características. La primera está relacionada con la geografía de la guerra, es decir, cuáles son sus nuevos dominios, que en este caso serán los cognitivos y tecnológicos relacionados con el ciberespacio. Las guerras de quinta generación hacen que la percepción de la mente humana sea el principal campo de batalla (Krishnan, 2022).

La segunda característica está relacionada con los actores (beligerantes y combatientes) y su naturaleza cambiante: cómo se van adaptando a los contextos sociopolíticos, económicos y tecnológicos.

> La guerra de quinta generación sugiere que los beligerantes podrían ser individuos o redes de pequeños grupos unidos por una ideología unificadora y tecnología avanzada. Una idea importante de la guerra de quinta generación es manipular a otros (apoderados) para que actúen en su nombre y confundir al adversario quién es el verdadero enemigo o incluso si están en un conflicto. (Krishnan, 2022, p. 24)

La tercera característica está enfocada en los objetivos que buscan estos actores y también cómo van cambiando en la guerra. El objetivo de estas guerras "no sería conquistar el Estado o dividirlo sino socavar el Estado. Si la guerra tiene éxito, el Estado objetivo habrá perdido su legitimidad hasta tal punto que no podrá estar seguro de la lealtad primaria de nadie" (Krishnan, 2022).

Finalmente, se encuentra lo que Reed denomina la fuerza: "una guerra moral y cultural que se libra mediante la manipulación de las percepciones y la alteración del contexto en el que se percibe el mundo" (Krishnan, 2022). El objetivo sería alterar la cultura o el entorno operacional de forma que favorezca los objetivos de los beligerantes, por eso el dominio cognitivo es fundamental (Krishnan, 2022).

Uno de los escenarios de las guerras de quinta generación son las ciudades. "De acuerdo con Dimarco (2012), los centros urbanos parecen haber dominado el campo de batalla durante la mayor parte de la historia, particularmente en la guerra premoderna" (Álvarez *et al.*, 2018, p. 194). La concentración sociodemográfica en las ciudades ha hecho que estas sean más proclives a conflictos, debido a los incentivos económicos y políticos que existen de atacar estos centros de gravedad (Álvarez *et al.*, 2018).

Por otra parte, otra de las características importantes de las guerras de quinta generación está relacionada con el nuevo dominio donde se libra la guerra: el ciberespacio. "Este es un dominio operacional moldeado por el uso de la electrónica y del espectro electromagnético para crear, modificar, guardar, intercambiar y explotar información a través de sistemas de interconexión e internet, y sus infraestructuras asociadas" (Piñeros *et al.*, 2020). En este caso, quien controle los flujos de información tiene mayores posibilidades de ganar la guerra. En ese sentido, el ciberespacio es el nuevo campo de batalla en el siglo XXI.

> Se experimenta una continua hostilidad entre diversos actores estatales y no estatales, conducidos en gran parte por medios no militares, como, por ejemplo, acciones de propaganda, agitación política, sabotaje, crimen, espionaje industrial y político, entre otros, llevados a cabo en, a través o en combinación con el ciberespacio. (Álvarez *et al.*, 2018, p. 201)

El ciberespacio tiene unas características especiales que generan unas ventajas asimétricas para los actores estatales y no estatales.

> El ciberespacio es un campo de batalla de grandes dimensiones y donde resulta relativamente fácil asegurar el anonimato, ya que además, los ataques se pueden lanzar desde casi cualquier parte del mundo; segundo, los efectos de los ataques son desproporcionados con respecto a su coste, es decir, las operaciones se pueden realizar sin necesidad de efectuar fuertes inversiones en recursos humanos y materiales; tercero, la naturaleza de los ciberataques fuerza a la mayoría de las víctimas, tanto reales como potenciales, a adoptar una actitud defensiva; cuarto, esta amenaza tiene un alcance global, en la cual el actor (ya sea ciberdelincuente, ciber-terrorista, etc.), puede operar desde cualquier parte del mundo con el único requisito de tener acceso al ciberespacio; y quinto, proporciona las herramientas necesarias para que los más pequeños puedan enfrentarse, incluso vencer y mostrarse superiores a los más poderosos, con unos riesgos mínimos para ellos. (Álvarez *et al.*, 2018, p. 201)

Es en este campo de batalla donde grupos de *hackers* como Anonymous han podido operar desde su creación en el año 2003. En este ciberespacio se puede generar un ciberconflicto que implica la confrontación entre dos o más partes, en donde los ataques se realizan en este nuevo domino de la guerra. Dicho ciber conflicto puede tener efectos devastadores, por ejemplo, en la infraestructura critica de un país, o en los sistemas de defensa de un país, entre otros. En ese sentido, el ciberespacio se convierte en un nuevo escenario de confrontación. "Las redes informáticas son susceptibles de recibir multitud de ataques distintos; éstos formarían parte de las amenazas que el ciberespacio puede tener que soportar como ámbito de comunicación y transmisión de información" (Agreda, 2012, p. 176).

Así mismo, a partir de la cuarta revolución industrial todos los procesos informáticos se han digitalizado, "el control que los sistemas cibernéticos ejercen sobre determinados procesos industriales y financieros proporciona un potencial inmenso de agresión desde el ciberespacio, aunque el objetivo esté situado fuera de él. Cabe enfatizar el riesgo a que están sometidos los servicios e infraestructuras críticos" (Agreda, 2012, p. 176).

Esto genera mayores vulnerabilidades a los Estados, porque toda la infraestructura crítica de un país está conectada en red, lo que la expone a un ciberataque. "Una infraestructura crítica es aquella que: 'su incapacitación o destrucción tendría un efecto debilitante en la seguridad, la economía nacional, la salud pública, o cualquier combinación de estos" (González, 2022). Por ejemplo, en 2010 Stuxnetc, un *software* malicioso logró dañar los motores de las centrífugas que se utilizan para el enriquecimiento de uranio del programa nuclear iraní. Igualmente, en 2015 en Ucrania, antes de la guerra con Rusia, se realizó un ciberataque que afectó la infraestructura eléctrica del país.

> Los *hackers* se infiltraron en tres compañías energéticas y cerraron temporalmente la generación de energía en tres regiones de Ucrania. Dejó a casi un cuarto de millón de personas sin electricidad hasta seis horas en pleno invierno. Los atacantes utilizaron el programa malicioso *BlackEnergy 3* para cerrar las tres subestaciones. Se cree que el programa malicioso se distribuyó mediante correos electrónicos de *phishing* personalizado, oculto en los archivos adjuntos falsos de Microsoft Office. (Mullane, 2019)

Por otra parte, en este ciberespacio todas estas acciones han generado que los dominios de la guerra se libren en un espacio digital, y se configure una ciberguerra (*cyberwar*), que se podría referir a la conducción y preparación de operaciones militares de acuerdo con los principios relacionados con la información.

> La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente se ha entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático que va desde la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computa-

dores, pasando por la planificación de las operaciones, la gestión del abastecimiento. (Sánchez, 2017, p. 111)

Esta ciberguerra está caracterizada por ser compleja, asimétrica, de corta duración, con un mayor espacio de combate, por la lucha por la superioridad de la información, entre otros. Ahora bien, los objetivos de esta guerra pueden variar desde el daño de un sistema o entidad, la interrupción de los flujos de información, la destrucción de la información, la reducción de la efectividad o eficiencia de los sistemas de comunicación del enemigo, impedir el acceso y la utilización de los sistemas o servicios críticos, entre otros (Sánchez, 2017). En este contexto, las redes sociales también se han convertido en un espacio de confrontación, sobre todo por la disponibilidad de información abierta que se puede rastrear.

Por otro lado, las guerras de quinta generación han implicado que los actores que participan en la contienda ya no sean solamente los Estados, y que estos que ostentan el monopolio legítimo de la violencia recurran al uso de las compañías militares de seguridad privada (CMSP). Algunos autores afirman que la presencia de las CMSP en los conflictos cuestiona la capacidad del monopolio legítimo de la violencia por parte del Estado, pero otros comparten la tesis de que la presencia de las CMSP no limita la capacidad estatal, sino que la amplía: "La industria militar y de seguridad privada es llamativa por su habilidad para ofrecer servicios militares de forma más eficiente, más rápidamente y mucho más barata de lo que las fuerzas militares estatales u otras compañías no militares podrían hacerlo" (Toro y Macías, 2012, p. 210). En casos de Estados fallidos, los CMSP pueden cumplir un rol de seguridad relevante para estabilizar las regiones (Toro y Macias, 2012). Igualmente, Macias menciona que "para preservar su monopolio sobre el uso legítimo de la fuerza, el Estado tiene entonces la facultad de delegar el uso de medios coercitivos en cualquier agente o institución que considere necesario, mientras asegure un control sobre ellas" (p. 51).

En 2019, el Pentágono gastó $370 mil millones en contratación, más de la mitad del gasto discrecional total relacionado con la defensa, $676 mil millones (Peltier, 2020). Así mismo, ese año hubo 53.000 contratistas estadounidenses frente a 35.000 soldados estadounidenses en el Medio Oriente. Desde el inicio de las operaciones en Afganistán en 2001, se estima que 8.000 contratistas estadounidenses han muerto, a comparación de los 7.000 soldados estadounidenses que han fallecido (Peltier, 2020). Estas cifras muestran la importancia que han tenido las compañías militares para los Estados Unidos y como el presupuesto destinado para esto ha sido bastante considerable.

Por otra parte, Urueña Sánchez (2018) señala que "el fenómeno de las CMSP hace parte de un proceso social más amplio y que tiene que ver con la constante progresión en la privatización de la seguridad. Este proceso afecta a la soberanía externa de los Estados, es decir sobre el no sometimiento a un poder superior" (p. 52). Por eso, los intentos de regulación en el sistema internacional han sido limitados, como se verá más adelante.

Las CMSP no solamente realizan actividades de provisión de armamento o de envío de personal entrenado para participar en los

conflictos, sino que también "han suministrado información e inteligencia a los gobiernos y empresas" (García, 2015). Así, las CMSP, conocidas como empresas de seguridad privada, ofrecen servicios de defensa y seguridad militar a gobiernos, organizaciones internacionales y empresas privadas.

Estas compañías proporcionan servicios como la protección de instalaciones, personal y equipos, la logística, el transporte de personal y material, la capacitación y asesoramiento en seguridad y defensa, la gestión de crisis, la seguridad marítima, entre otros servicios relacionados con la seguridad. Por ejemplo, en 2004, la empresa Black Water

> … ganó la licitación para la protección de personal de la embajada estadounidense en Bagdad a la vez que Triple Canopy hizo lo propio con la oficina diplomática en Basrah en ese mismo país. Estas mismas tres CMSP obtuvieron contratos para la segunda versión del WPPS cuyo valor estimado se tazó en 1200 millones de dólares por cinco años para la protección de personal en varias ciudades de Irak, Israel, Bosnia y Afganistán. (Urueña, 2020, p. 175)

A diferencia de los militares convencionales, las CMSP no están sujetas a la cadena de mando militar ni a la supervisión gubernamental directa y, por lo tanto, operan de manera independiente. Algunas CMSP han sido criticadas por su falta de transparencia y por actuar fuera de la ley en algunos casos, lo que ha llevado a preocupaciones sobre su papel en la seguridad global y la protección de los derechos humanos.

> Otro elemento fundamental a considerar frente al fenómeno de las compañías militares privadas es su nivel de regulación ¿Existe regulación frente a estas compañías? En primer, es posible señalar tres: prohibición, regulación o autorregulación. Los tres mecanismos han tratado de ser utilizados para establecer un control a las CMSP y la mayoría de las iniciativas en ese sentido han sido lideradas por el gobierno suizo, por la Cruz Roja y por un grupo de trabajo de Naciones Unidas que se creó inicialmente para revisar el fenómeno del mercenarismo pero que posteriormente se le agregó la función de analizar el comportamiento de las CMSP en el mundo. (Macías, s. f.)

Quizá el problema de las compañías militares es que el nivel de regulación gubernamental es difícil de conseguir, ya que se opera bajo una lógica corporativa que está exenta del control político y democrático, pero sobre todo jurídico, que se realiza a un Estado. De acuerdo con Macías (s. f.), al equipo de trabajo de Naciones Unidas se le encargó investigar el impacto de las CMSP. El grupo de trabajo creó un borrador de una convención internacional que regulaba el funcionamiento de esas empresas que fue entregado a la Comisión de Derechos Humanos de la ONU.

También existe el Documento de Montreux, que exhorta a los Estados para adquirir buenas prácticas en la contratación de CMSP en conflictos armados. Igualmente, "aconseja no contratar a este tipo de compañías para realizar actividades reservadas por el DIH a agentes o autoridades estatales, subrayando la necesidad de garantizar el cumplimiento de las normas del DIH y no colaborar en su infracción" (Urueña y Olasolo, 2022, p. 50).

En resumen, las guerras de quinta generación se caracterizan porque los escenarios de confrontación se han ampliado hacia dominios

cognitivos y tecnológicos, como el ciberespacio. Asimismo, los actores que pueden conducir la guerra ya no son necesariamente solo los Estados, porque aparecen las compañías militares de seguridad privadas que terminan por ejercer roles y misiones relacionadas con seguridad y defensa, y las ciudades se han convertido en los centros de gravedad de este tipo de guerras.

EL CONFLICTO ENTRE RUSIA Y UCRANIA

El conflicto entre Rusia y Ucrania, que comenzó en 2022, tiene antecedentes desde 2014. En el marco de la posguerra fría, en el año 2013 la Unión Europea y Ucrania iniciaron negociaciones para un acuerdo político y comercial que generó tensiones con Rusia, ante lo cual el presidente de Ucrania, Víktor Yanukóvich, suspendió las negociaciones y estallaron las famosas protestas "Euromaidan". En 2014, el parlamento ucraniano destituyó al presidente y Rusia, aprovechando la coyuntura, decide anexar la península de Crimea. Este acontecimiento marcó un punto de inflexión porque significó una derrota para Rusia. Sin embargo, Vladimir Putin aprovechó que la población de la península de Crimea, situada en el extremo sur de Ucrania, es mayoritariamente rusófona y tiene sólidos vínculos étnicos, culturales e históricos con Rusia, para llevar a cabo un referéndum exprés que concluyó en la independencia de Crimea y en su inmediata anexión por Rusia (Rosales, 2022).

La estrategia de Rusia frente a Ucrania, que se remonta al 2014, ha implicado una combinación de tácticas irregulares y urbanas, así como operaciones de desestabilización. Según Álvarez *et al.* (2018), Rusia ha utilizado una combinación de operaciones especiales, presión económica, agentes de inteligencia, manipulación del flujo de gas natural, ciberataques, guerra de información y uso de la fuerza militar convencional para ejercer presión y disuasión a fin de lograr sus objetivos políticos. Todo esto está perfectamente coordinado y forma parte de un plan de operaciones que podría denominarse "guerra híbrida".

Ahora bien, actualmente la tensión entre Rusia y Ucrania ha girado en torno a la adhesión de Ucrania a la Organización del Tratado del Atlántico Norte (OTAN). Para Rusia, una de sus mayores amenazas a la seguridad es la OTAN, en parte porque pone en riesgo el control de sus zonas de influencia histórica. "El documento Estrategia 2020 (de febrero de 2008) describió una visión del futuro de Rusia a largo plazo. La mayor amenaza para la seguridad nacional exterior de Rusia sería la OTAN y una cuestión fundamental, la seguridad energética y de los compatriotas en el espacio post soviético" (Milosevich, 2016, p. 9). Para entender las razones geopolíticas de la operación realizada por Rusia es importante señalar que:

> La política exterior y de seguridad de Rusia está impulsada por el empeño de recuperar el estatus de gran potencia mediante y el control de las "zonas de influencia" en los países vecinos, a través de un sofisticado proceso de "reimperialización" (entendido como resurgimiento o reconstrucción del imperio) así como mediante una escalada en la competición geopolítica con Occidente (la UE, EE. UU. y la OTAN). (Milosevich, 2016, p. 10)

Igualmente, en el documento de Estrategia de Seguridad Nacional de Rusia de 2021 se estableció que "los peligros y las amenazas militares a la Federación Rusa se han intensificado por los intentos de ejercer presión militar sobre Rusia, sus aliados y socios, y por el aumento de la infraestructura militar de la Organización del Tratado del Atlántico Norte cerca de las fronteras rusas" (Federación Rusa, 2021, p. 12). Por eso, cuando Ucrania manifestó su intención de ingresar a la OTAN, Rusia decide lanzar la "operación militar especial", ya que la OTAN representa una amenaza para su seguridad nacional.

Por otra parte, el 54% del territorio ocupado por Rusia ha sido reconquistado por Ucrania en los casi dos años desde la invasión en gran escala, mientras que Rusia sigue ocupando el 18% del país. La ofensiva ucraniana en 2023 logró avances territoriales menores, pero las líneas del frente han permanecido estables durante casi un año. El avance es cada vez más complicado debido a las posiciones fijas de ambos bandos, y se estima que el número de bajas militares ha llegado a medio millón. Mientras tanto, Rusia sigue bombardeando ciudades ucranianas y bloqueando sus puertos, y Ucrania ha intensificado los ataques con drones contra barcos e infraestructuras rusas (Global Conflict Tracker, 2024).

Desde 2022, Ucrania ha recibido casi 350.000 millones de dólares en ayuda, incluidos 77.000 millones de Estados Unidos. Los combates y los ataques aéreos han causado casi 22.000 víctimas civiles, mientras que 5,1 millones de personas están desplazadas internamente y 6,2 millones han huido de Ucrania; asimismo, 17,6 millones de personas necesitan ayuda humanitaria (Global Conflict Tracker, 2024).

Según el último reporte de la Oficina del Alto Comisionado para los Derechos Humanos de las Naciones Unidas (ACNUDH), entre el 1 de agosto y el 30 de noviembre de 2023, el conflicto causó 2.440 víctimas civiles (576 muertos y 1.864 heridos). Esto supone un descenso del 25% en comparación con los cuatro meses anteriores y del 46% en comparación con el mismo periodo de 2022. El descenso de víctimas civiles observado en 2023 puede atribuirse a varios factores, como la estabilización de la línea del frente, la evacuación de civiles de las zonas de conflicto y el refuerzo de los sistemas de defensa antiaérea en determinadas zonas, especialmente en Kiev (Office of the High Commissioner for Human Rights, 2023). Según Allison y Davidson (2023), "si bien la guerra interestatal promedio dura menos de dos años, las principales guerras rusas y estadounidenses desde la Segunda Guerra Mundial han durado más de una década, lo que sugiere que el conflicto entre Rusia-Ucrania podría durar muchos años más" (p. 16).

Desde sus inicios en febrero de 2022, el conflicto entre Rusia y Ucrania ha estado caracterizado por el control de las principales ciudades. La ofensiva inició por el control de Kiev, la capital de Ucrania, y otras ciudades de ese país. Sin embargo, para abril de 2022, la contraofensiva de Ucrania logró un retroceso estratégico de las fuerzas armadas rusas sobre todo en Kiev.

De esta manera, es posible evidenciar que el conflicto se concentró en las ciudades. Estas han sido golpeadas por ataques aéreos, misiles de crucero y balísticos e incluso artillería. Las

ciudades se configuran como centros de gravedad, porque concentran a la población civil, lo cual permite aumentar la presión política y militar del conflicto. Así mismo, se configuran otros centros de gravedad económicos y sociales como las centrales eléctricas y los hospitales, con los cuales se busca generar afectación a la población civil y aumentar la presión sobre el gobierno ucraniano.

La Oficina del Alto Comisionado para los Derechos Humanos de la ONU siguió documentando ataques de las fuerzas armadas rusas con muchas víctimas en zonas residenciales. Al menos 68 ataques con misiles y municiones lanzados por la Federación de Rusia contra objetivos en las provincias de Odesa, Zaporizhzhia, Donetsk, Mykolaiv, Chernihiv, Cherkasy, Sumy, Kyiv, Lviv, Khmelnytskyi y Poltava causaron la muerte de civiles y dejó numerosos heridos. En ese sentido, las acciones militares se siguen concentrando en las ciudades y zonas residenciales (Office of the High Commissioner for Human Rights, 2023). El siguiente mapa muestra el control territorial y las zonas en disputa en Ucrania.

Las ofensivas más significativas a las ciudades han implicado el ataque a hospitales, centrales eléctricas y nucleares vitales para el funcionamiento de una ciudad. Por ejemplo, en marzo de 2022 se realizó un ataque aéreo que afectó al hospital infantil y de maternidad de Maripol, que causó la muerte de tres personas, incluida una niña, y 17 personas heridas, entre ellas mujeres en estado de embarazo. En las dos primeras semanas de la invasión, los rusos lanzaron más de 40 ataques aéreos y con cohetes contra la propia ciudad de Zhitómir (BBC, 2022).

Un factor importante es que la estrategia de Rusia ha implicado ataques aéreos coordinados a varias ciudades al mismo tiempo. Por ejemplo, en abril de 2022 se realizaron ataques aéreos en Lviv y Dnipro, después de los fuertes bombardeos en Luhansk y Járkiv.

Otros ataques con los que se evidenció la afectación al funcionamiento de las ciudades fueron los efectuados contra centrales eléctricas y nucleares. En marzo de 2022, se realizó un ataque contra la central nuclear de Zaporizhzhia, ubicada a unos 200 kilómetros al oeste de la ciudad de Donetsk. Después, en julio de 2022, se realizó otro ataque a la central nuclear de Zaporiyia. La central nuclear de Zaporiyia es la mayor de Ucrania y de toda Europa. Según la empresa energética estatal Ukrenergo, del 50 al 60% de la electricidad de la red ucraniana se produce en plantas de energía nuclear (DW, 2022).

En septiembre se realizó un ataque contra una presa cerca de Kryvyi Rih y realizaron un ataque aéreo cerca de una central eléctrica en Mykolaiv. Las fuerzas rusas han lanzado ataques aéreos que afectan las infraestructuras civiles, según lo manifestó un alto funcionario militar de los Estados Unidos (CNN, 2022). En octubre de 2022, el ejército ruso lanzó 83 misiles contra Ucrania, de los cuales 43 fueron derribados por las fuerzas ucranianas. Según informes, al menos 14 personas murieron y casi 100 resultaron heridas (BBC, 2022).

En conclusión, la mayoría de los ataques aéreos y la ofensiva en general se ha concentrado hacia el control de las ciudades, porque representan centros de gravedad importantes en materia económica, social, energética y, por supuesto, política.

FIGURA 1. CONTROL TERRITORIAL DE RUSIA EN UCRANIA CON FECHA DE CORTE 1 DE FEBRERO 2024

Nota: el mapa muestra los territorios de Ucrania en disputa a fecha de corte de febrero de 2024. Rusia ha estado enfocada en la región del Donbas, y se ha mantenido en esa posición.

Fuente: Institute for the Study of War (2024).

Por otra parte, Ucrania ha estado sujeta a varios ciberataques desde el año 2015. En ese año, la red eléctrica de Ucrania sufrió un apagón energético a causa de un ataque cibernético: el BlackEnergy. El objetivo de este ataque fue el sabotaje de los sistemas de control de la red eléctrica, que interrumpió el suministro a 1,5 millones de habitantes en la región de Ivano-Frankivsk. Desde el año 2007, ha sido utilizado en ataques cibernéticos relacionados con la denegación de servicio y la amenaza persistente de avanzada. Este virus consiste,

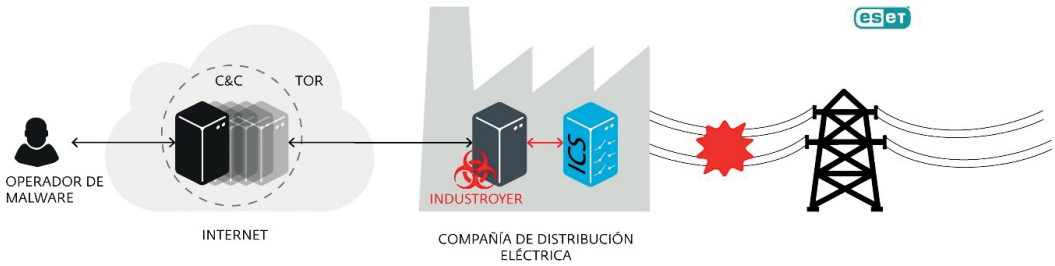
en términos generales, en la producción de ataques DoS, campañas de ciber-espionaje y destrucción de información.

Casi exactamente un año después del ataque BlackEnergy, el virus Industroyer provocó, nuevamente, un apagón durante una hora en Kiev, la capital del país (figura 2). Fue uno de los primeros virus diseñados específicamente para atacar una red eléctrica, porque posee la capacidad de provocar, a gran escala, un daño significativo sobre los diversos sistemas que empleen energía eléctrica. Este virus es un *malware* que puede controlar directamente a los interruptores presentes en una subestación eléctrica mediante protocolos de comunicación utilizados a escala global.

En el año 2017 se lanzó el ataque Petya, el *software* destructivo se ocultó en una actualización de un popular *software* de contabilidad utilizado en Ucrania, pero se extendió por todo el mundo destruyendo los sistemas informáticos de miles de empresas y causando daños por aproximadamente US$10.000 millones (BBC, 2022). Este virus es un *malware*[3] que codifica e infesta los sistemas operativos de Microsoft Windows, infectando los datos almacenados del disco duro; de esta manera, estos datos solo se desbloquean con la clave de cifrado; el ataque de NotPetya en un principio se encargó de subvertir la actualización del *software* opcional de contabilidad del gobierno ucraniano. En los ataques siguientes se infectaron con el *malware* las empresas ucranianas, los ministerios, bancos, empresas de electricidad, logrando un efecto espejo en Francia, Alemania, Italia, Polonia, Reino Unido, Australia y Estados Unidos. Es considerado el ataque cibernético más costoso de la historia.

Ahora bien, desde el inicio del conflicto, los ataques cibernéticos se incrementaron. Según la ONG suiza Cyberpeace Institute, a la fecha, contra Ucrania se han realizado 636 ataques y contra Rusia 331. Para el caso de Ucrania, los ataques DDoS representan el 89%

FIGURA 2. VIRUS INDUSTROYER



Nota: el gráfico muestra cómo funciona el virus Industruyer.

Fuente: tomado de Lameiras (s. f.).

[3] *Malware* es un término que abarca cualquier tipo de *software* malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable.

de todos los incidentes. Los sectores más atacados fueron la administración pública (19), los medios de comunicación (15), TIC (15), financiero (10) y comercio (8). Se reportó un ciberataque al equipo de respuesta de emergencias informáticas de Ucrania (CERT-UA) dirigido a una infraestructura energética crítica del país. Según el reporte del Cyberpeace Institute, los ataques cibernéticos han estado patrocinados por Rusia (Cyberpeace Institute, 2023).

En el tercer trimestre de 2023, el CyberPeace Institute registró un descenso de las ciber actividades maliciosas perpetradas por agentes de amenazas prorrusos contra entidades de Ucrania, en comparación con el trimestre anterior. El análisis del Instituto sugiere que Sandworm21 es probablemente el actor que genera mayor amenaza, con una afiliación prorrusa patrocinada por el Estado, que lleva a cabo operaciones maliciosas contra entidades ucranianas. Sandworm[4] es una amenaza persistente avanzada (APT) destructiva, activa desde 2009, atribuida a la Federación Rusa. Al menos desde 2009 ha estado vinculado a la Dirección Principal de Inteligencia del Estado Mayor de la Federación Rusa (Cyberpeace Institute, 2023).

Por otra parte, la participación a gran escala de actores no estatales ha determinado el uso de la cibernética en la guerra rusa contra Ucrania. Los actores estatales ya no son los únicos con capacidad ofensiva porque se ha reducido el umbral para llevar a cabo ataques. En los primeros días de las hostilidades, ambos países solicitaron el respaldo de individuos dispuestos a unirse a un "ciberejército" (Duguin y Pavlova, 2023). Por ejemplo, Mykhailo Fedorov, el viceprimer ministro de Ucrania, publicó un anuncio en sus redes sociales buscando crear un ejército IT ucraniano. Según el viceministro, la idea fue lanzar ciberataques contra bancos, empresas y entidades gubernamentales rusas, para generar desestabilización y caos a nivel digital, algo que los *hackers* de Putin llevan haciendo contra Ucrania desde meses antes de la invasión; de hecho, Rusia ha usado a Ucrania como fuente de entrenamiento para preparar los ataques digitales al resto de gobiernos del mundo (Otero, 2022).

Para el caso de Rusia, en el año 2022, el sector de las TIC fue el más atacado. La administración pública fue el segundo sector más atacado, seguido de los ataques contra el sector financiero. Por primera vez desde el inicio del conflicto, el CyberPeace Institute detectó varios ataques reivindicados por actores cibernéticos (*hackers*) contra entidades de la Federación Rusia (Cyberpeace Institute, 2022). Así mismo, "Kaspersky Lab detectó una campaña de ciberespionaje contra grandes empresas rusas. Un actor de amenazas desconocido llevó a cabo la campaña a través de correos electrónicos de *phishing* dirigidos a las empresas" (Cyberpeace Institute, 2022, p. 7).

El Ejército Nacional Republicano, un colectivo con base en Rusia que se opone al gobierno del presidente Putin, ha sido activo tanto en el mundo físico como digital,

[4] El grupo es responsable de varios ciberataques de gran repercusión, como los apagones eléctricos generalizados en Ucrania en 2015, y el *malware* NotPetya utilizado en 2017.

publicó su manifiesto en agosto de agosto de 2022. En el mundo físico, se han se han atribuido actividades de sabotaje como incendiar coches y centros de movilización. Este actor tomó crédito de dos ciberataques significativos, uno de ellos fue un *ransomware* contra una importante empresa rusa de rusa de desarrollo de software; y un ciberataque a la cadena de suministro contra empresas rusas de TIC que prestan servicios en el ámbito de la seguridad nacional al gobierno de la Federación Rusa. (Cyberpeace Institute, 2022, p. 7)

Así se puede evidenciar que los dos actores principales del conflicto (Rusia y Ucrania) han realizado ataques en el ciberespacio. Estos ciberataques son realizados en su mayoría por grupos de *hackactivistas.* En el caso ruso:

Eronen (2016) afirma que la conducta rusa aprovecharía la disposición de Vladimir Putin para actuar fuera de las normas operacionales de la posguerra, dentro de las cuales Occidente ha construido sus mecanismos de respuesta militar y política. El ciberespacio parece configurarse como uno de los principales teatros de la actividad asimétrica de Rusia. Esto se debería a que el ciberespacio ofrece una manera fácil de combinar los escenarios de combate, incluidos el espionaje, las operaciones de información y el combate convencional, realizándolo detrás de una barrera de denegabilidad plausible. Gracias al ciberespacio, un atacante puede cruzar sigilosamente grandes distancias, sin barreras físicas, y alcanzar un objetivo determinado. (Álvarez *et al.*, 2018, p. 220)

Otro aspecto importante por mencionar es que, paralelamente al inicio del conflicto, los ataques cibernéticos también fueron parte de la estrategia utilizada por Rusia en el marco del conflicto. Desde el comienzo de la invasión rusa de Ucrania el 24 de febrero de 2022, según un reporte de Microsoft, se han realizado ataques cibernéticos:

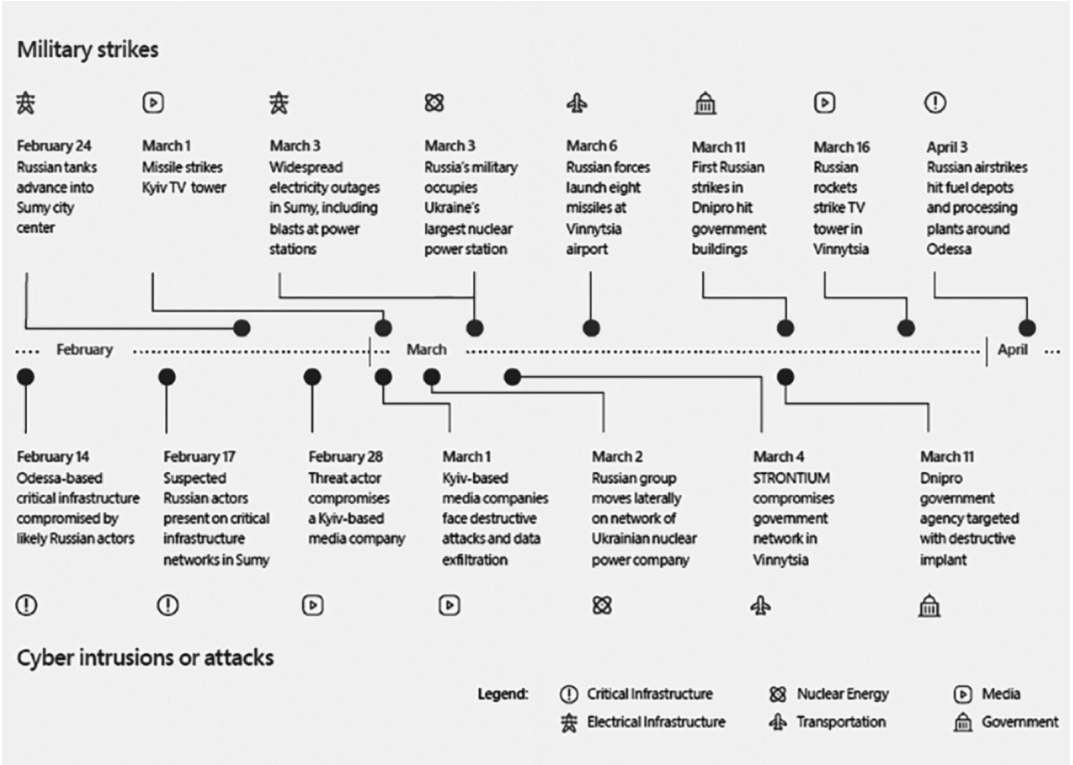
Se observó que grupos rusos de amenaza cibernética han realizado acciones en apoyo de sus objetivos estratégicos y tácticos. Una cronología de ataques militares e intrusiones cibernéticas muestra varios ejemplos de operaciones de redes informáticas y operaciones militares que parecen trabajar en tándem contra un objetivo común, aunque no está claro si hay coordinación centralizada de tareas o simplemente un conjunto común de prioridades comunes. Las operaciones hasta ahora han sido coherentes con las acciones para degradar, perturbar o desacreditar las funciones gubernamentales, militares y funciones económicas, asegurar puntos de apoyo en infraestructuras críticas, y reducir el acceso del público ucraniano a la información. (Microsoft Corporation, 2022)

En la figura 3 se observa cómo los ataques militares iban acompañados con ataques cibernéticos como parte de la estrategia militar.

Un ataque relevante fue realizado el 2 de marzo, donde se identificó a un grupo ruso en la red informática de la empresa de energía nuclear. Al día siguiente, los militares rusos atacaron y ocuparon la mayor central nuclear de la empresa. Durante la misma semana, el ejército ruso MSTIC, llamado Strontium, comprometió una red informática del gobierno en Vinnytsia y dos días después lanzó ocho misiles de crucero contra el aeropuerto de la ciudad (Microsoft Corportation, 2022).

Otro grupo hackctivista que ha participado en el conflicto es Anonymous. A principios de mayo, el colectivo de hacktivistas YourAnonSpider, afiliado a Anonymous, reivindicó

FIGURA 3. CRONOLOGÍA DE ATAQUES MILITARES Y CIBERATAQUES DURANTE EL INICIO DEL CONFLICTO ENTRE RUSIA Y UCRANIA



Nota: la imagen muestra los ataques militares y los cibernéticos realizados al inicio del conflicto.

Fuente: tomado de Microsoft Corportation (2022).

el pirateo de RuTube, que dejó fuera de servicio la plataforma de video rusa durante al menos dos días. Más o menos al mismo tiempo, NB65, otro grupo afiliado a Anonymous se atribuyó el ataque a los servidores de varias de las principales cadenas de televisión rusas y su desconexión (Canadian Centre for Cyber Security,2022). Anonymous alertó al gobierno ruso de los ciberataques, y coordinó a nivel internacional los ataques cibernéticos.

Por otra parte, la OTAN ha señalado que enfrenta una variedad de desafíos en los dominios de conflicto emergentes.

Estos dominios pueden surgir de la introducción de tecnologías nuevas y disruptivas. Los dominios del espacio y la cibernética, por ejemplo, surgieron de desarrollos en tecnologías de cohetes, satélites, computación, telecomunicaciones e interconexión de redes. El uso cada vez más generalizado de las redes sociales, la mensajería

social y las tecnologías de dispositivos móviles ahora está permitiendo un nuevo dominio: la guerra cognitiva. (Johns Hopkins University & Imperial College London, 2021)

Por otra parte, la guerra se libra también en las redes sociales y los medios de comunicación, que se convierten en herramientas para difundir propaganda y desinformar. Al respecto, para justificar la operación, desde que inició el conflicto las líneas discursivas manejadas por Rusia y sus medios de comunicación como RT (*Russian Today*) estaban relacionadas con el objetivo de desnazificar Ucrania. Según un estudio realizado por Briceño y Heaphy (2022):

En el caso de RT, se obtuvieron 36 publicaciones a lo largo del periodo de recopilación[5], en su mayoría, 41,7%, estos eran noticias que buscaban determinar un "héroe" y un "villano" dentro del conflicto (F4.4). La tendencia del medio eran titulares y *leads* que hablaban de ataques inminentes; ataques de banderas falsas en contra de civiles; incidentes de represión y desaparición en contra de opositores políticos y otros que criticaban a Volodymyr Zelensky; demonificación; e incidentes que linkean con el nazismo y neonazismo al estado y ejército ucraniano.

En uno de los primeros titulares de RT el 24 de febrero de 2024 se lee: "Putin decide realizar 'una operación militar especial' para defender Donbas". En el artículo se justifica la operación diciendo:

… el jefe de Estado explicó que la operación militar rusa se llevará a cabo en defensa propia contra quienes habían tomado a Ucrania como "rehén". Los acontecimientos de hoy no están relacionados con el deseo de atentar contra los intereses de Ucrania y del pueblo ucraniano, sino con la protección de la propia Rusia frente a quienes han tomado a Ucrania como rehén y tratan de utilizarla contra nuestro país y su pueblo. (RT, 2022)

Igualmente, por medios oficiales, como el Ministerio de Asuntos Exteriores de la Federación de Rusia, Serguéi Lavrov, justificó la operación: "se trata no solo de la situación en Ucrania, de la desmilitarización y desnazificación de este país, de la prevención del genocidio en su territorio, el cese de toda clase de violencia, de las garantías que les posibiliten a los ucranianos decidir ellos mismos su destino" (Ministerio de Asuntos Exteriores de la Federación Rusa, 2022).

Por otra parte, una cuenta de Twitter en 2022 publicó un video de 12 segundos que supuestamente muestra un ataque en la ciudad de Mariúpol en el este de Ucrania el 24 de febrero. El video decía "se registran bombardeos en Mariúpol, Ucrania se encuentra bajo ataque, el cual ha ganado decenas de miles de reacciones en redes. Sin embargo, enseña en realidad una tormenta eléctrica en la ciudad rusa de Volzhsk el 28 de junio de 2021, como comprobó la agencia EFE" (France 24, 2022).

En la guerra cognitiva, la mente humana se convierte en el campo de batalla. El objetivo es cambiar no solo lo que la gente piensa, sino también cómo piensa y actúa. En su forma extrema, tiene el potencial de fracturar y fragmentar a toda una sociedad, de modo que ya no

[5] Para el periodo del 4 de abril y el 4 de mayo de 2022.

tenga la voluntad colectiva de resistir las intenciones de un adversario. (Johns Hopkins University & Imperial College London, 2021).

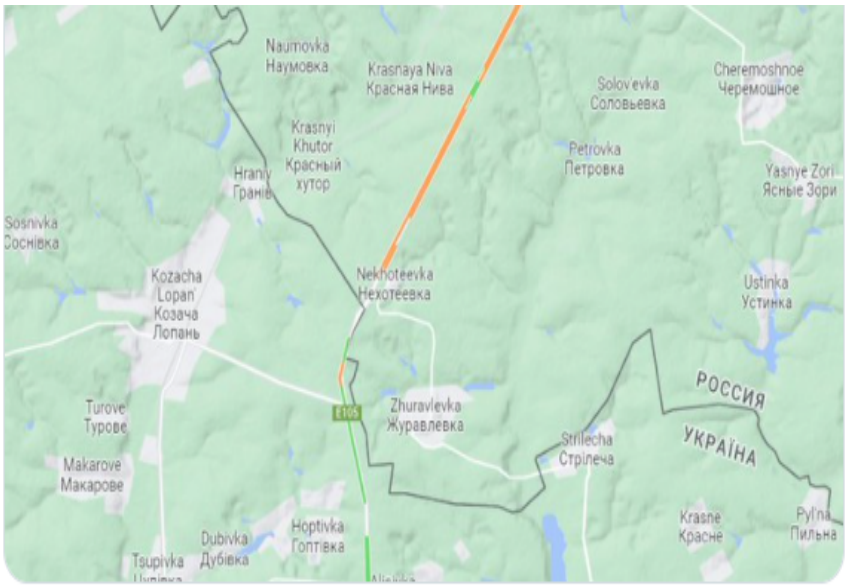
Igualmente, el uso de aplicaciones y herramientas tecnológicas como Google Maps han jugado un papel clave en el conflicto. Esta aplicación logró reportar el avance de los tanques rusos momentos previos al inicio del conflicto. Después, para evitar que las tropas rusas tuvieran información sobre las Fuerzas Militares de Ucrania, Google Maps desactivó esta opción (figura 4).

También, en abril de 2022, un usuario en Twitter (@Suriyakmaps) creó un mapa en Google Maps, que mostró no solo los frentes del conflicto, sino sus principales cambios (figura 5).

Por otro lado, en el conflicto entre Rusia y Ucrania, se han involucrado compañías militares privadas, como el grupo Wagner, que apoyó la estrategia de Rusia en Ucrania, y fue fundamental para mantener la acción ofensiva en el año 2022 y 2023. Las acciones de empresas privadas en muchas ocasiones son una proyección de los deseos geopolíticos del Estado al que pertenecen (Ballesteros, 2021). Las profundas conexiones de Wagner con los principales líderes políticos rusos distinguen a esta empresa de otras.

El personal de Wagner (5.000 soldados) está mayoritariamente compuesto por excombatientes de Asia Central, Cáucaso y los Balcanes, con experiencia en combate cuerpo a cuerpo, con problemas financieros y con

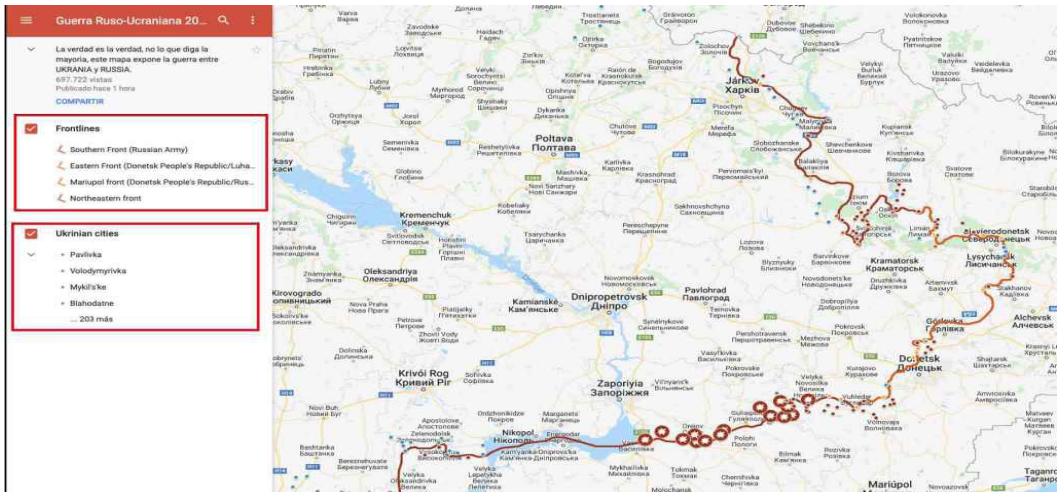
FIGURA 4. MAPA MOVIMIENTOS PREVIOS AL CONFLICTO ENTRE RUSIA Y UCRANIA



Nota: la imagen muestra en tiempo real en Google Maps, cómo se congestionó la carretera en Rusia antes de entrar a Ucrania.

Fuente: tomado de Lewis (2022).

FIGURA 5. GOOGLE MAPS CONFLICTO ENTRE RUSIA Y UCRANIA



Nota: el mapa consta de dos grandes grupos: los frentes bélicos que muestran los frentes marcados por las fuerzas rusas, los que delimitan las zonas del conflicto, las ciudades ucranianas y el paso de la guerra por ellas.

Fuente: tomado de Fernández (2022).

dificultades de adaptación a la vida social (Ballesteros, 2021).

El Grupo Wagner llevó a cabo por primera vez operaciones de combate en el sureste de Ucrania, en 2014. El periodista de investigación ruso Ruslan Leviev ha informado de que el Grupo Wagner participó activamente en la anexión ilegal de Crimea por parte de Rusia. En aquel momento, el Grupo Wagner estaba formado por un mosaico de diversos elementos, que iban desde los restos del Cuerpo Eslavo hasta voluntarios locales con motivos personales. En cualquier caso, mientras estuvo en Ucrania, el grupo operó principalmente en el territorio de la autoproclamada República Popular de Luhansk. (Sergey Sukhankin, 2018)

Por otra parte, el personal de Wagner ha operado en primera línea en todas las guerras recientes de Rusia en Ucrania y Siria. A veces han luchado junto al ejército ruso "oficial", a veces por su cuenta. Los operadores de Wagner han estado también en Libia y han tenido un rol más tradicional de capacitación y de seguridad en Sudán y la República Centroafricana (BBC Mundo, 2020). Rusia comenzó a retirar a sus soldados de varios países para llevarlos al frente ucraniano y servir de apoyo al ejército regular ruso (BBC, 2023).

Esta situación se ha acentuado especialmente después de que Rusia no alcanzara los objetivos militares iniciales como la toma de Kiev, y de que el conflicto se estancase. Además de la experiencia previa en combate, la presencia de Wagner en los frentes más violentos, como Bakhmut, permite a Moscú no contabilizar sus bajas como propias (BBC, 2023).

> Más de 30.000 miembros del Grupo Wagner han resultado heridos o muertos en Ucrania, según estimaciones de la Casa Blanca. De ellos, alrededor de 9.000 murieron en combate, según el portavoz del Consejo de Seguridad Nacional. Este grupo fue designado como un grupo delictivo transnacional por parte de Estados Unidos en enero de 2023. (Washington Post, 2023)

Así mismo, Rusia se ha enfrentado a una escasez de personal para enviar al frente de un conflicto. Aunque Putin ordenó una movilización parcial de las reservas el año pasado, muchos hombres rusos en edad militar huyeron del país, lo que obligó al Kremlin y a Wagner a recurrir a las cárceles en busca de reclutas (Washington Post, 2023).

El Ministerio de Defensa del Reino Unido mencionó que es probable que los combatientes de Wagner reclutados en prisión tengan un índice de bajas de alrededor del 50% en Ucrania. El ministerio calcula que se han registrado hasta 200.000 bajas combinadas entre las tropas rusas y las fuerzas mercenarias alineadas desde la invasión del 24 de febrero, con hasta 60.000 muertos entre ambas (Washington Post, 2023). Antes de la invasión rusa de Ucrania, se cree que el Grupo Wagner solo contaba con unos 5.000 combatientes.

El Grupo Wagner ha estado muy implicado en los esfuerzos rusos por capturar la ciudad de Bajmut en el este de Ucrania. Las tropas ucranianas afirmaron que se ha enviado a combatientes del Grupo Wagner a atacar en gran número en campo abierto. Después de que Rusia afirmara haber capturado la ciudad de Soledar, cerca de Bajmut, estalló una disputa entre su Ministerio de Defensa y el Grupo Wagner sobre quién debía llevarse el mérito. Los fiscales ucranianos acusan a tres mercenarios del Grupo Wagner de haber matado y torturado a civiles cerca de Kiev en abril de 2022, junto con tropas rusas regulares (BBC, 2023).

Finalmente, al igual que Rusia, otros Estados autocráticos como China, Corea del Norte, Venezuela o Nicaragua estarían mejor posicionados para desenvolverse en las guerras de quinta generación, porque, como tomadores de decisiones centralizadas, pueden actuar rápidamente, sin obstáculos y frenos impuestos por controles democráticos como un poder legislativo (Álvarez *et al.*, 2018), comparado con Estados democráticos que tienen que respetar la separación de poderes.

En junio de 2023 se generaron tensiones entre el líder del Grupo Wagner y el Ministerio de Defensa ruso, a tal punto que Yevgueni Prigozhin movilizó tropas de su grupo, llamando a iniciar un conflicto civil armado contra Rusia. Después de un acuerdo con el gobierno ruso para irse a Bielorrusia, Prigozhin murió en un accidente en avión.

CONCLUSIONES

Las guerras de quinta generación se caracterizan porque los escenarios de confrontación se han ampliado hacia dominios cognitivos y tecnológicos, como el ciberespacio. Igualmente, los actores que pueden conducir la guerra ya no son necesariamente solo los Estados, porque aparecen las compañías militares de seguridad privadas, que terminan por ejercer roles y misiones relacionadas con la seguridad y la defensa, y las ciudades se han convertido en los centros de gravedad de este tipo de guerras.

Además, este conflicto de quinta generación ha evolucionado y uno de los campos de confrontación es el espacio cognitivo, donde los actores que participan en ella buscan estrategias para controlar los flujos de información de la opinión pública para mantener la legitimidad de las guerras.

El conflicto entre Rusia y Ucrania se puede catalogar como un conflicto de quinta generación porque la confrontación que se presenta en todos los dominios de la guerra también ha implicado que se libre en el ciberespacio. El ciberespacio se declara como el quinto dominio de la guerra (tierra, aire, espacio, mar y ciberespacio) por los riesgos y las amenazas que su uso masivo genera y la dependencia tecnológica que existe. Uno de los grandes riesgos de realizar un ataque cibernético es que su alcance puede ser global, como efectivamente sucedió con el ataque de NotPetya, que ha sido catalogado como uno de los ciberataques más costosos de la historia.

De esta manera, los actores utilizan estrategias cibernéticas para atacar a su adversario, acompañadas de estrategias convencionales militares, como sucedió cuando realizaron un ciberataque a una de las plantas nucleares en Ucrania, y después se produjo una operación militar para tomar el control físico de la planta nuclear.

Uno de los objetivos estratégicos trazados por Rusia era tener un control territorial de las principales ciudades de Ucrania como Kiev. De esta manera, una guerra de quinta generación se libra en varios dominios (tierra, mar, aire, espacio y ciberespacio), pero las batallas se concentran en las ciudades porque son los centros de gravedad que albergan a la población civil, y se genera una mayor presión hacia los Estados cuando estas son atacadas. Los ataques han sido dirigidos a las principales ciudades de Ucrania, lo que ha afectado las infraestructuras críticas como la energía, plantas nucleares, entre otros. En varios casos, se han atacado bienes civiles que son protegidos por el derecho internacional humanitario, como lo fue el ataque aéreo al hospital materno-infantil en Mariúpol.

Por otra parte, el conflicto ha implicado que compañías militares de seguridad privada como el Grupo Wagner tengan una alta responsabilidad en el conflicto. Con el beneplácito del gobierno ruso, el Grupo Wagner reclutó a ciudadanos rusos en las cárceles para cubrir el déficit de personal militar. Finalmente, los conflictos de quinta generación tienden a extenderse en el tiempo, como está sucediendo con Rusia y Ucrania.

REFERENCIAS

Agreda, J. R. (2012). El ciberespacio como escenario de conflictos. Identificación de las amenazas. *El ciberespacio. Nuevo escenario de confrontacion*. Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=4540376

Álvarez, C. E., Santafé, J. F. y Urbano, O. J. (2018). *Metamorphosis Bellum*: ¿mutando a guerras de quinta generación? En *Escenarios y desafíos de la seguridad multidimensional en Colombia.* Escuela Superior de Guerra.

Allison,G y Davidson,K . (2023). *Russia-Ukraine war report card.* Harvard Kennedy School Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/russia-ukraine-report-card

Ballesteros, J . (2021). Empresas militares y de seguridad privada: entre el logro de la seguridad y la lesión de bienes jurídico-penales. *Revista Crimininalidad, 63*(1). http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082021000100123&lng=en&tlng=es.

Barrera, S , *et al*. (2021). Ética militar en el marco de guerras de quinta generación: propuestas teóricas para reestructurar la educación en instituciones militares. En *Ética militar y nuevas formas de guerra. Retos para las Fuerzas Armadas colombianas* (cap. 7). Escuela Superior de Guerra.

BBC Mundo (2020). Cómo opera el Grupo Wagner, el "brutal" ejército privado de mercenarios rusos. *BBC Mundo*. https://www.bbc.com/mundo/noticias-internacional-53344507#:~:text=Los%20operadores%20de%20Wagner%20han,plan%20fracas%C3%B3%20en%20gran%20medida.

BBC (2023). What is Russia's Wagner Group of mercenaries in Ukraine? *BBC Mundo*. https://www.bbc.com/news/world-60947877

BBC Mundo (2022). Rusia bombardea Kyev y otras ciudades de Ucrania en la más amplia oleada de ataques en meses. *BBC Mundo*. https://www.bbc.com/mundo/noticias-internacional-63198535

Briceño, D. y Heaphy, C. (2022). *Cobertura del conflicto entre Rusia y Ucrania. De los medios digitales de BBC, CNN y RT en el periodo del 4 de abril al 4 de mayo del 2022.* Universidad del Desarrollo. https://repositorio.udd.cl/server/api/core/bitstreams/2c26712d-4893-4b32-9794-fcbd8bc68bd1/content

Canadian Center for Cybersecurity (2022). Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine. https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf

CNN (2022). Los rusos siguen realizando ataques aéreos que "impactan en lasinfraestructuras civiles de Ucrania" según militar estadounidense. *CNN*. https://cnnespanol.cnn.com/2022/09/20/ultimas-noticias-guerra-rusia-ucrania-orix-51/

Cyberpeace Institute (2022). Cyber Dimensions of the armed conflict in Ukraine. *Ciberpeace Institute*. https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf

Cyberpeace Institute (2023). Cyber Dimensions of the armed conflict in Ukraine. *Ciberpeace Institute* https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf

DW (2022). ¿Cuán importante es la central nuclear de Zaporiyia para Ucrania? *DW*. https://www.dw.com/es/cu%C3%A1n-importante-es-la-central-nuclear-de-zaporiyia-para-ucrania/a-62976821

Duguin, S. y Pavlova P. I. (2023). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. Directorate-general for external policies policy department*. European Parlament https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf

Expósito, I. O. (2012). La naturaleza comparativa de los estudios de caso. Una revisión politológica sobre el estado de la cuestión. *Encrucijadas: Revista Crítica de Ciencias Sociales* (4), 2174-6753. https://dialnet.unirioja.es/servlet/articulo?codigo=4193111

Federación Rusa (2021). National Security Strategy of Russian Federation https://paulofilho.net.br/wp-content/uploads/2021/10/National_Security_Strategy_of_the_Russia.pdf

Fernández, M. (2022, abril 25). El mapa de Google Maps para seguir los movimientos de Rusia en su invasión a Ucrania. *El Español*. https://www.elespanol.com/omicrono/software/20220425/google-maps-seguir-movimientos-rusia-invasion-ucrania/667683315_0.html

France 24 (2022). El crucial papel de la desinformación en la invasión rusa a Ucrania. *France 24*. https://www.france24.com/es/rusia/20220225-guerra-ucrania-desinformacion-noticias-falsas

Gajat, M. (2018). Reflexiones sobre la guerra asimétrica a través de la historia. *Revista Latinoamericana de Estudios de Seguridad*, *24*(1), 204-220 dx.doi.org/10.17141/urvio.24.2019.3522

García, J. (2015). El papel de los mercenarios en los conflictos internacionales: de la Grecia clásica a las compañías militares privadas de hoy. *Analecta polit, 5*(8), 169-182. https://revistas.upb.edu.co/index.php/analecta/article/view/2506

González, S. (2022). *Ciberataques a la infraestructura crítica de un país y sus consecuencias.* We live Security. https://www.welivesecurity.com/la-es/2022/03/10/ciberataques-infraestructura-critica-pais-consecuencias/

Global Conflict Tracker (2024). War in Ukraine. https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine

Institute for the Study of War (2024, febrero 1). I. Russian offensive campaign assessment. https://understandingwar.org/backgrounder/russian-offensive-campaign-assessment-february-1-2024

Johns Hopkins University y Imperial College London (2021). *NATO.* Countering cognitive warfare: Awareness and resilience. *Nato Review*. https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

Krishnan, A. (2022). Fifth generation warfare, hybrid warfare, and gray zone conflict: A comparison. *Journal of Strategic Security*, *15*(4), 14-31. https://www.jstor.org/stable/48707883

Lind, W. (1989). El rostro cambiante de la guerra. *Marine Corps Gazette*.

Lind, W. (2005). Comprendiendo la guerra de cuarta generación. *Military Review*.

Lameiras, A. (s. f.). Industroyer: una amenaza cibernética que derribó una red eléctrica. Welivesecurity.com. https://www.welivesecurity.com/la-es/2022/06/13/industroyer-amenaza-ciberneticaderribo-red-electrica/

Lewis J . (@Armas controlwonk) Febrero 23, 2022 Traffic Jam (Tweet) Twitter.

Macías, A. (s. f.). *Memorias del Seminario Academico "Prospectivas en Seguridad y Defensa en Colombia"*. Escuela Superior de Guerra. https://issuu.com/maestriaenseguridadydefensanacional/docs/memorias_20seminario_20prospectivas

Macías, A. (2012). The impact of PMSC on the role of today`s military. *Revista Opera*, 12, 221-238.

Microsoft (2022a). *Defending Ukraine, early lession from the cyber war.* Microsoft Corporation. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

Microsoft Corporation (2022b). *An overview of Russia's cyberattack activitu in Ukraine.* Microsoft Corporation. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Milosevich, M. (2016). *El proceso de "reimperialización" de Rusia, 2000-2016.* Documento de trabajo. Real Instituto El Cano. https://www.realinstitutoelcano.org/documento-de-trabajo/el-proceso-de-reimperializacion-de-rusia-2000-2016/

Ministerio de Asuntos Exteriores de la Federación Rusa (2022). *Entrevista ofrecida por el ministro de Asuntos Exteriores de la Federación de Rusia, Serguéi Lavrov, a las cadenas RT, NBC News, ABC News, ITN, France 24 y China Media Group*, *Moscú, 3 de marzo de 2022.* Ministerio de Asuntos Exteriores de la Federación Rusa. https://mid.ru/es/foreign_policy/rso/1802677

Mullane, M. (2019). Ciberataques dirigidos a infraestructuras críticas. *Revista de la Normalizacion Española*. https://revista.une.org/15/ciberataques-dirigidos-a-infraestructuras-criticas.html

Murillo, J. (s. f). *Estudio de Caso.* Universidad Autonoma de Madrid. https://www.academia.edu/27844895/_Estudio_de_casos_Asignatura_M%C3%A9todos_de_la_investigaci%C3%B3n_educativa_Profesor

Office of the High Commissioner for Human Rights (2024). Report on the human rights situation in Ukraine. https://www.ohchr.org/en/documents/country-reports/report-human-rights-situation-ukraine-1-august-30-november-2023

Otero, C. (2022). *IT Army, el ciber-ejército de hackers del gobierno ucraniano convocados por Telegram.* Betech. https://as.com/meristation/2022/03/15/betech/1647351141_355985.html

Peltier, H. (2020). *The Growth of the "Camo Economy" and the Commercialization of the Post-9/11 Wars.* Watson Institute International Public Affairs. https://watson.brown.edu/costsofwar/papers/2020/growth-camo-economy-and-commercialization-post-911-wars-0

Piñeros *et al.* (2020). La ciberseguridad, la ciberdefensa, la identidad y los intereses nacionales y las Fuerzas Militares de Colombia. En E. Pastrana, S. Reith, F. Cabrera (Editores). *Identidad e intereses nacionales de Colombia.* Fundación Konrad Adenauer, Escuela Superior de Guerra.

Rosales,E. (2022). El conflicto Rusia-Ucrania. Antecedentes, contexto y perspectivas. *Revista UNAM, 5*. https://revista.unaminternacional.unam.mx/nota/2/el-conflicto-rusia-ucrania-antecedentes-contexto-y-perspectivas

RT (2022). Putin decide realizar "una operación militar especial" para defender Donbass. *Rt en Español.* https://actualidad.rt.com/actualidad/421170-putin-decide-realizar-operacion-militar-especial-donbass

Sánchez Flores, F. A. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: consensos y disensos. *Revista Digital de Investigación en Docencia Universitaria*, *13*(1), 102-122. https://dx.doi.org/10.19083/ridu.2019.644

Sánchez, G. (2017). Ciberguerra y ciberterrorismo. En A. e. al, *Amenazas pasadas presentes y futuras: las guerras asimétricas.* Universidad Santo Tomás.

Sukhankin, S. (2018). *Continuing War by Other Means': The Case of Wagner, Russia's Premier Private Military Company in the Middle East.* The Jamestown Foundation. https://jamestown.org/program/continuing-war-by-other-means-the-case-of-wagner-russias-premier-private-military-company-in-the-middle-east/

Toro, M. P. y Macías, A. (2012). Las compañías militares y de seguridad privada en Estados fallidos: ¿una solución a la incapacidad estatal? *Opera 12*(12), 205-219

Urueña-Sánchez , M. y Olasolo Alonso, H. (2022). Las compañías militares y de seguridad privadas: hacia una definición operativa para el derecho internacional humanitario. *Revista Criminalidad*, *64*(2), 47-61. https://doi.org/10.47741/17943108.354

Urueña Sánchez, M. I. (2018). Las compañías militares y de seguridad privada: ¿El comienzo del fin de los Estados? *Civilizar*, *18*(34), 51-60. https://doi.org/10.22518/usergioa/jour/ccsh/2018.1/a03

Urueña Sánchez, M. (2020). *Mercenarios y compañias militares y de seguridad privadas.* Tirant lo Blanch.

Valle, J. (2022). El conflicto en Ucrania: guerra híbrida e intervención militar convencional. *Revista Seguridad y Poder Terrestre, 1*(1), 62-76. https://doi.org/10.56221/spt.v1i1.7

Washington Post (2023). Over 30,000 Wagner Group fighters killed or injured in Ukraine, U.S. says. *Washington Post*. https://www.washingtonpost.com/world/2023/02/18/wagner-group-ukraine-war-casualties/