Escenarios Actuales, año 30 N°1, abril, 2025, pp. 35-52
Centro de Estudios e Investigaciones Militares
Santiago de Chile
ISSN 0717-6805

Guerra híbrida y amenazas: hechos y tendencias

Gonzalo Arré Duarte[1]

Resumen

En este artículo se analizan las tendencias de la guerra híbrida en conflictos contemporáneos, destacando como principales características: el uso de diversos instrumentos de poder, la simultaneidad de los modos de combate y la consecución de objetivos estratégicos. Se explora cómo las empresas privadas, la dependencia económica y las tecnologías digitales juegan roles cruciales en los conflictos modernos. Se examinan casos como el uso de la red Starlink en Ucrania, la dependencia europea del gas ruso y los ciberataques que afectan infraestructuras críticas, para ilustrar las tendencias en amenazas híbridas y su impacto en la seguridad global.

Abstract

This article analyzes hybrid warfare trends in contemporary conflicts, highlighting its main characteristics: the use of various instruments of power, the simultaneity of combat modes, and the achievement of strategic objectives. It explores how private companies, economic dependence, and digital technologies play crucial roles in modern conflicts. Cases such as the use of the Starlink network in Ukraine, European dependency on Russian gas, and cyberattacks affecting critical infrastructures are examined to illustrate trends in hybrid threats and their impact on global security.

Palabras clave
Guerra híbrida
Empresas privadas
Dependencia económica
Tecnologías digitales
Ciberataques
Infraestructuras físicas

Keywords
Hybrid war
Private companies
Economic dependence
Digital technologies
Cyberattacks
Physical infrastructures

Introducción

En el siglo XXI, la guerra híbrida se ha convertido en una de las formas de conflictos más usuales. Lo conflictos combinan tácticas de guerra convencional con técnicas no convencio-

1 Cientista Político, Pontificia Universidad Católica de Chile. Magíster en Ciencia Política, con mención en Relaciones Internacionales, Pontificia Universidad Católica de Chile.

nales para alcanzar objetivos estratégicos. Valeri Gerasimov[2] en su discutido ensayo de 2013, "The Value of Science is in the Foresight", expresa que "…*las reglas de la guerra han cambiado. El valor de los medios no-militares para lograr los fines políticos y estratégicos no solo se han incrementado, sino que en algunos casos excede la efectividad de las armas*".[3] Este enfoque descrito por Gerasimov ilustra la anexión de Crimea en 2014, donde Rusia combinó el uso de fuerzas militares convencionales con tácticas de guerra informacional y el apoyo a fuerzas separatistas.

Cabe mencionar que el término guerra híbrida gana popularidad después de la Segunda Guerra del Líbano en 2006.[4] En aquella oportunidad Hezbolá, combinó tácticas convencionales y de guerrilla que denotan algunos elementos por los que hoy se conoce la guerra híbrida: la combinación de operaciones convencionales, insurgencia, tácticas de guerrilla, guerra psicológica, terrorismo, actividades criminales, dio muestra una nueva forma de conflicto, sin restricciones antes conocidas y excediendo todo límite de derecho internacional.[5]

Paralelamente, hay quienes sostienen que las guerras híbridas no son una novedad del siglo XXI, sino una constante en la evolución de los conflictos humanos. Williamson Murray y Peter R. Mansoor en su obra "Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present", analizan nueve estudios de caso que tienen características representativas de la guerra híbrida a lo largo de los últimos dos milenios.[6]

En la misma línea, se puede mencionar una frase de Sun Tzu, en El arte de la guerra, escrito en el siglo V antes de Cristo, que tiene relación a lo que se ha comentado:

"*Utiliza generalmente fuerzas directas para iniciar la batalla y fuerzas indirectas para lograr que esta se decida a tu favor. Los recursos de quiénes son hábiles en la utilización de las fuerzas indirectas son tan infinitos como los de los Cielos y de la Tierra, y tan inagotables como el curso de los grandes ríos*".[7]

En este sentido, claramente por fuerzas directas se entiende los medios militares, y por contraste, por fuerzas indirectas implícitamente se encuentra un incipiente proto concepto de guerra híbrida, en tanto se hace uso de otros medios como la diplomacia, la economía o la información.

2 Jefe del Estado Mayor General de las Fuerzas Armadas rusas desde 2012. Se atribuye a su pensamiento militar influencia en la estrategia rusa. Desde principios de 2023 fue nombrado responsable militar en Ucrania. Revisar: BBC News. "Profile: Russia's new military chief Valery Gerasimov". BBC News. 11 de enero de 2012. [en línea]. Disponible en: https://www.bbc.com/news/world-europe-20270111; Europa Press. "Rusia cambia al comandante de operaciones en Ucrania". Última Hora. 11 de enero de 2023. [en línea]. Disponible en: https://www.ultimahora.es/noticias/internacional/2023/01/11/1861653/guerra-ucrania-cambio-comandante-rusia.html

3 GERASIMOV, Valeri. "The Value of Science is in the Foresight: The New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," trans. by Robert Coalson, Military-Industrial Kurier, February 2013. [en línea] disponible en: http://usacac.army.mil.

4 Si bien la expresión es más antigua, no fue hasta noviembre de 2005 cuando adquirió mayor trabajo académico en un artículo del general James N. Mattis y del teniente coronel Frank G. Hoffman. MATTIS, James N. & HOFFMAN, Frank. Future warfare: The rise of hybrid wars. Proceedings-United States Naval Institute, 131(11). 2005., pp. 18-19.

5 *Ibídem*.

6 MURRAY, Williamson, and MANSOOR, Peter R. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge University Press, 2012.

7 TZU, Sun, y ÁLVAREZ, Ricardo. El arte de la guerra. Buenos Aires: Prometeo Libros, 2016.

Otro debate conocido, ha sido sobre el concepto de "guerra híbrida", si representa una innovación en la forma y desarrollo de los conflictos bélicos o si simplemente deriva de términos ya existentes, como guerra asimétrica, cibernética, irregular, guerra no lineal, medidas activas o conflicto en "la zona gris".[8] A pesar de estos dos debates, con las características expuestas, la guerra híbrida se presenta como un fenómeno esencialmente contemporáneo, por ello las podemos trabajar desde la base de los elementos comunes presentes en las distintas definiciones y conceptualizaciones.

Como hemos visto, la naturaleza de los conflictos presenta formas más complejas que en el pasado, como resultado de estas revoluciones tecnológicas e informativas crearon nuevos medios y áreas de confrontación que no estaban previamente disponibles. Tanto las nuevas tecnologías, como las nuevas tácticas muestran tendencias de la evolución de los conflictos, las que no son del todo nuevas, ya que reflejan las dinámicas ya existentes. No obstante, subrayan que el impacto de los desafíos híbridos solo aumentarán y se presentarán de formas novedosas.

Recientemente, en el año 2024, un análisis prospectivo realizado por The Hague Centre for Strategic Studies (HCSS) y Netherlands Organisation for Applied Scientific Research (TNO), basado en una revisión bibliográfica de fuentes de origen diverso, identificó cinco tendencias principales en el panorama de amenazas hibridas globales: la explotación de las tendencias económicas, la digitalización como arma, la distorsión de la realidad, la manipulación de la polarización social y la diversificación de herramientas y actores.[9]

Dentro de este marco, es de interés en este artículo profundizar en tres tendencias. La primera, el uso de empresas privadas como actores híbridos. Este fenómeno ocurre como una forma de diversificar los actores y herramientas de amenaza hibrida. empresas tecnológicas pueden colaborar, ser cooptadas o creadas para desempeñar un rol en conflictos híbridos. La segunda, se destaca por el uso de la dependencia económica como arma. Finalmente, pero no menos importante, la utilización tecnologías digitales para socavar la infraestructura en el mundo físico.

La evolución del concepto de guerra híbrida

La guerra ha sido una constante en la historia de la humanidad, adaptándose y cambiando según las condiciones y necesidades de cada época.[10] A lo largo de las generaciones, sus formas y métodos han evolucionado para cumplir con los objetivos y visiones de quienes gestionan estos conflictos.

En las últimas décadas, el modo dominante del conflicto ha excedido "*a los enfrentamientos militares de fuerza contra fuerza guiados por los principios*

8 CAPDEVILLA, Claudia Antonella. "Guerra Híbrida: las nuevas tecnologías como instrumento de guerra". CEERI Global, Año 1. Número 2. diciembre 2022. Buenos Aires, Argentina. [en línea]. Disponible en: https://www.ceeriglobal.org/wp-content/uploads/2023/01/Revista-CEERI-Global-N2-1-59-75.pdf

9 Esta revisión bibliográfica incluye fuentes de la Unión Europea, América del Norte, Ucrania, Rusia, Japón y China. Extraído desde: ROMANSKY, Sofia; HOENIG, Alisa; MEESSEN, Rick, & KRUIJVER, Kimberley. New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape. The Hague Centre for Strategic Studies and TNO, 2024.

10 VON CLAUSEWITZ, Karl. De la guerra. Santa Fé, Argentina: El Cid Editor, 2003.

tradicionales de hacer la guerra".[11] De esta forma, ya no se impone la propia voluntad al enemigo, no existe desarme, tampoco sometimiento a alguna norma jurídica, incluso en algunos casos no hay lucha armada.

Lo anterior, ha llevado a asumir que nos encontremos en una nueva era en que el término guerra ha adquirido una dimensión bastante más amplia. La denominación de guerra asimétrica, guerra irregular, guerra compuesta, guerra sin restricciones, guerra no lineal o guerra cibernética –que no son foco de este artículo– han surgido para identificar con mejor nitidez a algunos de los tipos de guerra que han proliferado en los últimos 50 años.

La primera conceptualización como tal de guerra híbrida, se encuentra en el trabajo de Frank Hoffman, que en su obra Conflict in the 21th Century. The Raise of Hybrid Wars (2007) señala que:

"*Las guerras híbridas incorporan un conjunto de diferentes formas de hacer la guerra que incluyen capacidades convencionales, formaciones y tácticas irregulares, actos terroristas incluyendo la violencia indiscriminada y la coerción y el desorden criminal*".[12]

Este concepto también abarca modalidades de guerra irregular como insurgencia, agitación, propaganda, guerrilla urbana, así como acciones convencionales limitadas, pero altamente eficaces. Además, se emplean armamentos avanzados y sofisticados de mando y control. Según Hoffman, las organizaciones analizadas tienden a ser más cohesionadas y tener mayores ambiciones políticas que los grupos insurgentes tradicionales. Así también, utilizan redes para difundir sus mensajes políticos a nivel global y mantienen relaciones con el crimen organizado internacional, lo que les proporciona financiamiento y acceso a bienes y servicios necesarios para sus operaciones.

Desde la OTAN, durante las primeras dos décadas de este siglo se han desarrollado diversos estudios para analizar la guerra híbrida, caracterizados por una aproximación comprensiva al concepto. Al concluir la Cumbre de Varsovia en julio de 2016, el comunicado de la OTAN destaca la "adaptabilidad de los medios utilizados", como un factor importante de la guerra hibrida.[13]

Posteriormente, la alianza atlántica a través del "The Hybrid Threats and Hybrid Warfare Reference Curriculum (HTHWRC)", adoptó un enfoque multidisciplinario donde acoge una idea mucho más extensa del concepto como:

"*El uso creativo del poder duro, blando e inteligente por parte de actores estatales o no estatales malignos para lograr objetivos bélicos y metas políticas. Los actos malignos incluyen un amplio espectro de instrumentos militares y no militares de poder coercitivo más allá del espacio de batalla multidominio concebido convencionalmente. La guerra híbrida abarca la política, la diplomacia, la información, la economía, la tecnología, el ejército y la sociedad, así como dimensiones como la cultura, la psicología, la legitimidad y la moral. La ejecución coordinada*

11 MAZARR, Michael J. Extremism, Terror and the Future of Conflict. 2006. [en línea]. Disponible en: https://www.hoover.org/research/extremism-terror-and-future-conflict

12 HOFFMAN, Frank. Confict in the 21st Century: The Rise of Hybrid Wars. Virginia, Estados Unidos, Potomac Institute for Policy Studies, 2017, p. 14.

13 Comunicado de la Cumbre de Varsovia. 2016. Delegación de Francia ante la OTAN. [en línea]. Disponible en: https://otan.delegfrance.org/Warsaw-Summit-Communique-2016.

de estos actos malignos ocurre tanto abierta como encubiertamente en las ambiguas zonas grises de interfaces borrosas: entre guerra y paz, amigos y enemigos, relaciones internas y externas, civiles y militares, y actores estatales y no estatales, así como en campos de responsabilidad generalmente por debajo del umbral de la guerra o como acompañamiento de un conflicto armado más regular".[14]

Por el lado de la Unión Europea, el comunicado de prensa de la Comisión Europea del 6 de abril de 2016, aborda la guerra híbrida, destacando que estas amenazas combinan métodos convencionales y no convencionales "*que pueden ser utilizados de forma coordinada por actores estatales o no estatales, operando por debajo del umbral de una guerra formal*". Donde su objetivo es causar daños directos, explotar vulnerabilidades, desestabilizar sociedades y crear ambigüedades que dificulten la toma de decisiones.[15]

España ha otorgado relevancia a la guerra híbrida desde principios de la década de 2010. Desde la Directiva de Defensa Nacional 2012 que menciona la amenaza híbrida, hasta la Estrategia de Seguridad Nacional de 2017, que se refiere al conflicto híbrido y la acción híbrida. Este último documento destaca como se combinan "*medios militares con ataques cibernéticos, elementos de presión económica o campañas de influencia en las redes sociales*".[16] Adicionalmente, el Concepto de empleo de las Fuerzas Armadas 2017, de marzo de dicho año, considera que la guerra híbrida "*nos obligan a aproximaciones globales para resolver las crisis, de baja o alta intensidad, en diferentes espacios físicos, virtuales, psicológicos o de opinión*".[17]

Finalmente, es su famosa cita "*en el siglo XXI, la línea entre la guerra y la paz ha sido borrada*"[18], Gerasimov nunca hace uso del concepto de guerra híbrida textualmente. Sin embargo, lo que hace en su planteamiento es atribuir las características de este fenómeno a Occidente, especialmente EE. UU. ha empezado estrategias no militares para desestabilizar naciones y expandir su influencia, utilizando levantamientos prodemocráticos y la "Primavera Árabe" como ejemplos. En lugar de operaciones, evitando conflictos directos entre potencias y empleando acciones no militares para alcanzar sus objetivos, lo que perjudica a Rusia y altera el balance de poder global.[19]

Esta propuesta de Gerasimov, ha evolucionado con los años, ha establecido que la nueva estrategia rusa debe integrar "poder duro" y "poder blando" por medio de una mezcla amplia y coordinada de herramientas convencionales y no convencionales, incluidas las militares, diplomáticas y económicas. Este enfoque busca minimizar el uso de elementos cinéticos, prefiriendo los no cinéticos, y explotar la acción indirecta, campañas de información, organizaciones militares privadas,

14 NATO. 2024. "Hybrid Threats and Hybrid Warfare". [en línea]. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf

15 Comisión Europea. 2016. "La Comisión Europea adopta el nuevo Paquete de Medidas sobre la Migración". [en línea]. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_16_1227.

16 Gobierno de España. Estrategia de Seguridad Nacional (ESN). 2017. [en línea]. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/documents/2017-1824_estrategia_de_seguridad_nacional_esn_doble_pag.pdf.

17 Ministerio de Defensa de España. Concepto de Empleo de las Fuerzas Armadas Españolas. 2017. [en línea]. Disponible en: https://www.defensa.gob.es/ume/Galerias/Descargas/legislacion/CONCEPTO-DE-EMPLEO-DE-LAS-FAS-ESPANOLAS-2017.pdf

18 GERASIMOV, *op. cit.*

19 BAQUÉS, Josep. "La Zona Gris: El nuevo terreno en juego". Revista "Ejércitos", Nº12. noviembre 2019. Zaragoza, pp. 11-12.

fuerzas de operaciones especiales y grupos de protesta interna.[20]

De acuerdo a lo señalado, la construcción teórica de lo híbrido incluye características que son variadas y dispares a la vez, dentro de las más relevantes se sobresalen las siguientes:[21]

- Los actores involucrados: desde Estados interviniendo de manera directa o delegando su actuación a agentes domésticos o proxies, hasta guerrillas, terroristas, redes criminales o contratistas militares privados.

- Uso combinado de medios militares y no militares: incluye tanto capacidades convencionales como tácticas irregulares, insurgencia, terrorismo, desórdenes criminales, ciberataques, ocultación y engaño o propaganda multicanal.

- Ambigüedad y zonas grises: las acciones híbridas operan en la ambigüedad, dificultando la distinción entre guerra y paz, y entre actores estatales y no estatales.

- Enfoque multidimensional: incluye dimensiones políticas, económicas, informativas, tecnológicas, militares y sociales.

- Coordinación y sincronización: las operaciones híbridas son altamente coordinadas, integrando diversos métodos y herramientas para maximizar el impacto.

- Herramientas utilizadas: desde armas sencillas empleadas de manera novedosa, sistemas sofisticados, armamento pesado, tecnologías de la información o nuevas tecnologías como material bélico.

- Fuentes de financiamiento: desde actividades legales y delictivas con estrecha colaboración con el crimen organizado y financiamiento oculto de los Estados.

- Enfoque de la OTAN: subraya la adaptabilidad de los medios utilizados en la guerra híbrida y la necesidad de un enfoque comprensivo para abordarla.

- Perspectiva de la UE: enfatiza que las amenazas híbridas buscan causar daños directos, desestabilizar sociedades y explotar vulnerabilidades.

- Enfoque ruso según Gerasimov: destaca el uso de poder duro y blando, integrando herramientas convencionales y no convencionales, y explotando la acción indirecta y campañas de información.

Empresas híbridas

En la guerra híbrida, el uso de empresas privadas como actores híbridos ha ocurrido como una forma de diversificar los actores y herramientas de amenaza hibrida.[22] Empresas pueden operar, colaborar, ser cooptadas o creadas para desempeñar un rol en conflictos híbridos.

20 ADAMSKY, Dmitry. "Cross-Domain Coercion: The Current Russian Art of Strategy." Proliferation Papers 54. Institut Français des Relations Internationales (Ifri). Noviembre2015, p.23.

21 CAPDEVILLA, Claudia Antonella. "Guerra Híbrida: las nuevas tecnologías como instrumento de guerra". CEERI Global, Año 1. Número 2. diciembre 2022. Buenos Aires, Argentina. [en línea]. Disponible en: https://www.ceeriglobal.org/wp-content/uploads/2023/01/Revista-CEERI-Global-N2-1-59-75.pdf ; ADAMSKY, Dmitry. *Op. cit.*

22 ROMANSKY, Sofia; HOENIG, Alisa; MEESSEN, Rick, & KRUIJVER, Kimberley. New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape. The Hague Centre for Strategic Studies and TNO, 2024.

Este término comprende tanto empresas de seguridad privadas como empresas civiles originalmente ajenas a la guerra. Sobre las del primer tipo, llevan bastante tiempo jugando un rol en conflictos híbridos. En contraposición, las del segundo tipo han jugado un rol menos definido o su inclusión total en conflictos híbridos data de menos tiempo.

Un caso bien documentado es el de Chiquita Brands International, una reconocida multinacional bananera, que enfrentó investigaciones debido a sus pagos a grupos paramilitares en Colombia entre 1997 y 2004. Estos pagos, fueron realizados a través de su filial en el país, C.I Banadex, alcanzaron 1.7 millones de dólares y tenían como objetivo garantizar la seguridad de sus operaciones y empleados en regiones como Urabá, donde operaban las Autodefensas Unidas de Colombia (AUC).[23]

Este caso pretérito ilustra cómo las empresas multinacionales pueden convertirse en actores indirectos de conflictos armados debido a las dinámicas locales de violencia y extorsión. Ballvé, argumenta que las estrategias paramilitares e intereses económicos de este tipo de empresa contribuyeron a la consolidación de modelos de control territorial que fortalecieron tanto la economía ilícita como las estructuras de poder local.[24] Este es un ejemplo que muestra la compleja relación entre empresas y conflictos, y cómo sus acciones pueden influir en las dinámicas de guerra y paz en regiones vulnerables.

En África, a lo largo de los años, la Royal Dutch Shell ha estado involucrada en una relación compleja con las comunidades locales y el gobierno nigeriano. Durante los 90s, Shell proporcionó apoyo logístico y financiero al gobierno nigeriano que reprimió brutalmente las protestas de la comunidad ogoni contra la explotación petrolera.[25] Este apoyo culminó con la ejecución de nueve activistas ogoni en 1995. Las acciones de Shell evidencian cómo una empresa civil puede influir significativamente en conflictos internos mediante la colaboración con actores estatales.[26]

El Instituto Mabna, establecido en Irán alrededor de 2013, inicialmente funcionó como una empresa privada destinada a ayudar a universidades e instituciones de investigación de Irán a acceder a recursos científicos no iraníes. Según una investigación de FBI, este instituto participó en un esquema masivo de robo de información, atacando más de cien mil cuentas de académicos y empleados del sector privado alrededor del mundo así como diversas organizaciones gubernamentales y no gubernamentales dentro

23 Aunque estos pagos se justificaron como una medida necesaria para la seguridad, eran ilegales bajo las leyes de EE. UU. que prohíben transacciones con organizaciones designadas como terroristas. En 2007, Chiquita se declaró culpable de estos cargos y recibió una multa de 25 millones de dólares del Departamento de Justicia de EE. UU., enfrentando consecuencias legales que incluyeron demandas civiles por parte de las familias de las víctimas de la violencia paramilitar conectada a sus pagos: NIETO, Paulo Felipe, y SUDARSKY, Juan Bernardo. "El caso de los pagos de Chiquita Brands a los paramilitares en Colombia durante el período 1997-2004: Un análisis de stakeholders". Universidad de los Andes, noviembre de 2007.; BUNSE, Simone, & COLBURN, Forrest. "Chiquita en Colombia". Academia, Revista Latinoamericana de Administración, (43), 2009, pp. 1-12.

24 BALLVÉ, Teo. Everyday State Formation: Territory, Decentralization, and the Narco Landgrab in Colombia. Environment and Planning D: Society and Space, 30(4), 2012, pp. 603-622. [en línea]. Disponible en: https://doi.org/10.1068/d4611

25 OKONTA, Ike, & DOUGLAS, Oronton. Where vultures feast: Shell, human rights, and oil in the Niger Delta. San Francisco: Sierra Club Books. 2001., pp. 1-286.; OKONTA, Ike. Behind the Mask: Explaining the Emergence of MEND Militia in Nigeria's Oil-Bearing Niger Delta. Institute of International Studies, University of California, Berkeley. 2006.

26 *Ibídem*.

de los Estados Unidos, la ONU, y el Fondo de las Naciones Unidas para la Infancia (UNICEF).[27]

Aunque el Instituto Mabna estaba inicialmente impulsado por una agenda independiente, su relación con el Cuerpo de la Guardia Revolución Islámica (IRGC) lo convirtió en un aliado y proxy,[28] llevando a cabo instrucciones cibernéticas a gran escala a cambio de beneficios financieros. Este tipo de operaciones cibernéticas es un ejemplo significativo de un actor no estatal que combina operaciones de hacking patrocinada por el Estado con funciones de hacker por encargo, se enmarcan en un contexto más amplio de amenazas hibridas.[29]

En el conflicto de Ucrania, tanto Google como Microsoft han desempeñado roles que destacan su creciente influencia en las relaciones internacionales a través de acciones que van más allá de las tradicionales prácticas empresariales. Según Matania y Sommer en el artículo "Tech titans, cyber commons and the war in Ukraine: An incipient shift in international relations", estas acciones no solo muestran su papel como nuevas potencias en las relaciones internacionales, sino que también reflejan una tendencia hacia la creciente independencia de estas compañías en una esfera tradicionalmente dominada por los Estados. [30]

Google, por ejemplo, comprometió 55 millones de dólares para apoyar a Ucrania, destinando fondos a organizaciones humanitarias y a esfuerzos para contrarrestar la información rusa en plataformas como YouTube y Google Play. Entre las iniciativas implementadas, se encuentra la creación de alertas de bombardeos en dispositivo de Android y la desactivación de funciones de tráfico en Google Maps, con el objetivo de proteger a comunidades locales, utilizando tecnología de detección de terremotos. Además, la empresa ha colaborado con el gobierno ucraniano para lanzar un sistema de advertencia de seguridad, incrementar las protecciones de seguridad en sus cuentas, y proporcionar accesos a servicios gratuitos Google Cloud y Google Translate para ayudar a los refugiados.

Por su parte, Microsoft desempeñó un papel crucial en el ámbito de la ciberseguridad. La compañía detectó y respondió al malware ruso (como FoxBlade) antes de que causara daño significativo, utilizando su programa Microsoft Defender para proteger a Ucrania de estos ataques y eliminar campañas de desinformación. Además, ha establecido una línea de comunicación directa con el gobierno de Ucrania para compartir inteligencia sobre amenazas y trasladando datos gubernamentales a la nube para protegerlos contra ataques. La empresa gastó aproximadamente 100 millones de dólares en ayuda, comparable al apoyo de algunos países europeos en términos de seguridad y asistencia

27 JOKINEN, Janne; NORMARK Magnus and FREDHOLM, Michael. "Hybrid Threats from Non-State Actors: A Taxonomy," Hybrid CoE Research Reports (The European Centre of Excellence for Countering Hybrid Threats, June 9, 2022, Report 6, [en línea]. Disponible en: https://www.hybridcoe.fi/wpcontent/uploads/2022/06/Hybrid-Coe-Research-Report-6-WEB-EDS-20221121.pdf.

28 Es un actor estatal o no estatal externo a la dinámica de un conflicto existente, donde son elegidos para ser el conducto para las armas, el entrenamiento y la financiación del benefactor para llevar a cabo acciones indirectas y evitar la identificación directa del principal. MUMFORD, Andrew."Proxy Warfare and the Future of Conflict."The RUSI Journal 158 (2): 2013., pp. 40–46. [en línea] Disponible en: doi:10.1080/03071847.2013.787733.

29 JOKINEN, Janne; NORMARK Magnus and FREDHOLM, Michael. *op. cit*.

30 MATANIA, Eviatar., & SOMMER, Udi. Tech titans, cyber commons and the war in Ukraine: An incipient shift in international relations. International Relations. 2023. [en línea]. Disponible en: https://doi.org/10.1177/00471178231211500

humanitaria. También, han interrumpido sus servicios en Rusia en respuesta a las sanciones.

En la misma línea, desde el inicio de la invasión rusa, Ucrania ha utilizado más de 42.000 terminales de Starlink los cuales han sido cruciales para las operaciones militares y la comunicación, permitiendo desde la coordinación de ataques hasta la realización de videoconferencias.[31] La capacidad de Starlink para mantener la conectividad incluso en áreas afectadas por ataques cibernéticos resta su importancia en un entorno bélico donde la comunicación y el acceso a la información son vitales.

Sin embargo, las decisiones de Elon Musk, CEO de SpaceX, de limitar el acceso a los servicios en ciertas situaciones, y su solicitud al pentágono para financiar el servicio, plantean cuestiones sobre la dependencia de las Fuerzas armadas de la tecnología privada y los riesgos involucrados, dado que tal dependencia puede convertirse en un peligro para la seguridad nacional.[32]

Dependencia económica

Como segundo punto, otra tendencia interesante a destacar es el uso de la dependencia económica como arma. Este fenómeno, si bien es de larga data, con la expansión del comercio y la mayor interdependencia económica, puede traer consigo distintos efectos.

La dependencia de Europa, y en particular de Alemania, del gas ruso ha sido un tema de preocupación, especialmente en el contexto de la invasión rusa a Ucrania en 2022. Alemania, como el mayor importador de gas ruso, se enfrentó a una interdependencia económica significativa, lo que complicó su política energética y su postura frente a Moscú. Antes de la crisis, Rusia era responsable de aproximadamente 36% de todas las importaciones de gas natural hacia la UE y un 45% de sus importaciones de carbón.[33]

Alemania, como el principal importador de gas ruso, se encontró en una posición vulnerable debido a su alta dependencia de este recurso. La red de gasoductos, como Nord Stream 1 y 2 era fundamental en esta relación, dado que representaba una vía crítica para estas importaciones y fue construida con el fin de eludir posibles conflictos a través de Ucrania.[34] Esta diversificación de rutas fue vista como un intento por parte de Rusia de asegurar su influencia no solo en la economía alemana, sino

31 SATARIANO, Adam; REINHARD, Scott; METZ, Cade; FRENKEL, Sheera & KHURANA, Malika. "With Starlink, Elon Musk's Satellite Dominance Is Raising Global Alarms." The New York Times, July 28, 2023. [en línea]. Disponible en: https://www.nytimes.com/interactive/2023/07/28/business/starlink.html.

32 KIM, Victoria, "Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack," The New York Times, September 8, 2023, [en línea]. Disponible en: https://www.nytimes.com/2023/09/08/world/europe/elonmusk-starlink-ukraine.html; MARQUARDT, Alex, "Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab." CNN, October 12, 2022; SITARAMAN, Ganesh, & PASCAL, Alex, "The National Security Case for Public AI". Vanderbilt Policy Accelerator: Vanderbilt University. 2024. [en línea]. Disponible en: https://cdn.vanderbilt.edu/vu-URL/wp-content/uploads/sites/412/2024/09/27201409/VPA-Paper-National-Security-Case-for-AI.pdf

33 BOEHM, Lasse & WILSON, Alex. "EU energy security and the war in Ukraine: From sprint to marathon". EPRS (European Parliamentary Research Service). Febrero de 2023. [en línea]. Disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739362/EPRS_BRI(2023)739362_EN.pdf

34 ADOMEIT, Hannes. Germany, the EU, and Russia: The Conflict over Nord Stream 2. Centre for European Studies (European Union Centre of Excellence [EUCE] at Carleton University). 2016. [en línea]. Disponible en: https://carleton.ca/ces/wp-content/uploads/Adomeit-policy-brief.pdf

también como una herramienta para presionar políticamente a Europa.[35]

Siguiendo esta línea, la influencia de Rusia en el suministro energético no solo tuvo implicaciones económicas. Utilizó su posición como proveedor dominante para ejercer presión política sobre países europeos, en lo que se conoce como una "arma" energética.[36] Este tipo de manipulación se observa cuando Rusia recurrió a aumentos de precios o amenazas de interrupciones en el suministro como tácticas de presión.[37]

Con el inicio de la guerra en Ucrania, el año 2022, el aumento en tarifas y la incertidumbre sobre la fiabilidad de Rusia como proveedor llevaron a un llamado urgente para reducir la dependencia del gas ruso. El Parlamento Europeo demandó la eliminación de esta dependencia e impulsó sanciones severas contra Rusia, incluyendo embargos sobre carbón y petróleo.[38] Sin embargo, la transición lejos del gas ruso no es sencilla. A pesar de que la UE logró diversificar sus fuentes de gas mediante el aumento de importaciones de gas natural licuado (GNL), la dependencia sigue presente en diversas formas.[39]

En otro orden de ideas, la diplomacia pública china ha emergido como una herramienta crucial en el conflicto entre Beijing y Taipei, en el marco del conflicto híbrido que se desenlaza bajo la política de "Una sola China". Este paradigma considera a Taiwán y a China continental como partes inseparables de un todo. El uso de la "diplomacia de chequera" es emblemático de este enfoque estratégico, que tiene como propósito disminuir el reconocimiento internacional de Taiwán mediante la combinación de incentivos económicos e influencia política –muestra de aquello la Belt and Road Iniciative– utilizando la ayuda exterior como un medio para persuadir a los receptores de cerrar o limitar cualquier representación oficial taiwanesa.[40]

La creciente influencia de la RPC en América Latina y el Caribe, donde se encuentran siete de los doce países que reconocen a Taiwán, subraya la importancia de esta región en el conflicto.[41] Los esfuerzos de Beijing por asegurar reconocimiento diplomático en el hemisferio a menudo involucran la promesa de inversiones significativas y ayudas económicas, desincentivando así la cooperación de estos países con Taiwán.[42] El "costo de Taiwán", como

35 KORTEWEG, Rem. Energy as a tool of foreign policy of authoritarian states, in particular Russia. Policy Department for External Relations. European Parliament. 2018. [en línea]. Disponible en: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2018)603868; WÓJTOWICZ, Anna. "EU Energy Security After Russia's Invasion of Ukraine – Substance, Strategy and Lobbying". Studia Europejskie - Studies in European Affairs 2/2024, pp. 157-171.

36 BROWN, Sierra. "Russia's Use of the Energy Weapon: How Russia Manipulates Ukraine, Georgia, and the Baltic States," Scholarly Horizons: University of Minnesota, Morris Undergraduate Journal: Vol. 6: Iss. 1, Article 1. 2019. [en línea]. Disponible en: https://doi.org/10.61366/2576-2176.1073

37 KORTEWEG. *Op. cit.* pp. 20-22.

38 BOEHM & WILSON, *Op. cit.*

39 *Ibídem*.

40 RICH, Timothy S. "Status for Sale: Taiwan and the Competition for Diplomatic Recognition." Issues & Studies 45 (2009): 159-188.; ZHANG, Denghua, & SMITH, Graeme. "China's Foreign Aid System: Structure, Agencies, and Identities." Third World Quarterly, 38 (10), 2017., pp. 2330–46. [en línea]. Disponible en: doi:10.1080/01436597.2017.1333419.

41 MALACALZA, Bernabé. What led to the boom? Unpacking China's development cooperation in Latin America. World Affairs 182(4): pp. 370–403. 2019. [en línea]. Disponible en: doi:10.1177/0043820019883251

42 RODRÍGUEZ, Mario Esteban. La batalla diplomática de Beijing y Taipei en América Latina y el Caribe. Revista CIDOB d'Afers Internacionals. 81: 2008, pp.209-231.

lo denominan algunos académicos, ilustra las repercusiones económicas que enfrentan los países al no reconocer a China, reflejando la presión que Beijing ejerce en la región para consolidar su dominio diplomático a través del uso estratégico de recursos económicos.[43]

Más recientemente, la "Health Silk Road", y la diplomacia de las vacunas durante la pandemia son dos estrategias diplomáticas que refuerzan el objetivo de Beijing de disminuir el reconocimiento internacional de Taiwán. El estudio de 2022 de Telias y Urdinez sobre "diplomacia de las mascarillas" concluye que la política de Una China afectaba fuertemente a las donaciones tanto taiwanesas como chinas.[44] Al ofrecer asistencia en salud pública y distribuir vacunas, China ha buscado mejorar su imagen y aumentar la confianza en su liderazgo global, mientras que algunos países, como Honduras y Paraguay, reconsideran sus vínculos con Taiwán en favor de acercamientos más favorables a China.[45]

Tecnologías digitales para socavar las infraestructuras físicas

La digitalización y el uso de tecnologías han transformado el panorama de la guerra híbrida, especialmente en la forma en que se pueden llevar a cabo ataques contra infraestructuras críticas. Los ciberataques pueden alcanzar el umbral de un "uso de la fuerza" cuando su escala y efectos son comparables a los de una operación militar convencional, pero la dificultad de atribuirlos a un actor estatal específico complica la respuesta de los Estados afectados.[46] La digitalización de infraestructuras críticas, como redes eléctricas y sistemas de telecomunicaciones, crea vulnerabilidades que pueden ser explotadas por actores estatales y no estatales para desestabilizar sociedades y erosionar su capacidad de defensa.[47]

Además, el creciente uso de tecnologías digitales en la defensa y los sistemas de infraestructura presenta un terreno fértil para las técnicas de guerra híbrida. La integración de vehículos autónomos y sistemas de inteligencia artificial en operaciones de espionaje subacuático permite a los actores encubiertos monitorear y preparar ataques a largo plazo contra infraestructuras críticas, que son fundamentales no solo para la seguridad nacional, sino también para la estabilidad económica.[48] Al combinar la dependencia económica con el sabotaje físico, estos actores pueden crear una red de influencia y control que socava la capacidad

43 LONG, Tom & URDINEZ, Francisco. Status at the margins: why Paraguay recognizes Taiwan and shuns China. Foreign Policy Analysis 17(1): 2021., pp. 1–22 [en línea]. Disponible en: doi:10.1093/fpa/oraa002

44 TELIAS, Diego, & URDINEZ, Francisco. China's Foreign Aid Political Drivers: Lessons from a Novel Dataset of Mask Diplomacy in Latin America during the COVID-19 Pandemic. Journal of Current Chinese Affairs, 51(1), 2022., pp. 108-136. [en línea]. Disponible en: https://doi.org/10.1177/18681026211020763

45 BARHAM, Elena, DALY, Sarah Z., GEREZ, Julian E., MARSHALL, John & POCASANGRE, OSCAR. "Vaccine Diplomacy: How COVID-19 Vaccine Distribution in Latin America Increases Trust in Foreign Governments." World Politics 75, N° 4 (2023): pp. 826-875. [en línea]. Disponible en: https://dx.doi.org/10.1353/wp.2023.a908776.

46 FINLAY, Lorraine, & PAYNE, Christian. "The Attribution Problem and Cyber Armed Attacks," American Journal of International Law. Vol. 113 2019: p. 203, [en línea]. Disponible en: https://doi.org/10.1017/aju.2019.35.

47 FIOTT, Daniel. "Digitalisation and Hybrid Threats: Assessing the Vulnerabilities for European Security," Hybrid CoE Papers (The European Centre of Excellence for Countering Hybrid Threats, paper 13, April 2013 [en línea]. Disponible en: https://www.hybridcoe.fi/wpcontent/uploads/2022/04/20220404-Hybrid-CoE-Paper-13-Digitalization-and-hybrid-threats-WEB.pdf.

48 ROMANSKY, Sofia; HOENIG, Alisa; MEESSEN, Rick, & KRUIJVER, Kimberley. op.cit.

de respuesta de un Estado frente a retaliaciones o agresiones directas.[49]

Rusia ha utilizado tecnologías digitales como parte de su estrategia de guerra híbrida para socavar la infraestructura física en Ucrania y otros países. Los ciberataques rusos han estado dirigidos a infraestructuras críticas como redes eléctricas, bancos y sistemas gubernamentales. Un ejemplo notable es la operación WhisperGate en Ucrania en enero de 2022, diseñada para destruir datos y paralizar sistemas informáticos clave antes de la invasión rusa.[50]

El uso estratégico del ciberespacio por parte de Rusia también ha incluido ataques a infraestructuras esenciales para la vida cotidiana y la economía de un país. Un caso emblemático fue el ataque a la red eléctrica de Ucrania en 2015 y el intento de sabotaje en 2022, llevado a cabo por el grupo APT Sandworm, vinculado a la inteligencia militar rusa.[51] Con anterioridad, en 2007, Rusia llevó a cabo un ciberataque masivo contra Estonia, paralizando servicios gubernamentales y bancarios como represalia por la retirada de un monumento soviético en Tallin.[52]

El desarrollo de inteligencia artificial (IA) también ha sido un componente clave en la estrategia cibernética rusa. Rusia ha invertido significativamente en ciberseguridad impulsada por IA para influir en la opinión pública y política a nivel mundial, como se evidenció en las operaciones de la Agencia de Investigación de Internet (IRA) y la Dirección Principal de Inteligencia del Ejército Ruso (GRU) durante las elecciones presidenciales de Estados Unidos en 2016.[53]

En esta línea, otro elemento clave de la estrategia rusa es el uso de la desinformación en plataformas digitales, para sembrar discordia y socavar la confianza en instituciones democráticas en Occidente. Ejemplos de ello fue para las elecciones en Estados Unidos y Europa, mediante la manipulación de redes sociales y el uso de "troll farms" para difundir narrativas favorables al Kremlin.[54] Este tipo de operaciones forman parte de la Doctrina Gerasimov, que enfatiza el uso combinado de medios militares y no militares para alcanzar objetivos estratégicos sin necesidad de un enfrentamiento directo.

Por otro lado, Corea del Norte ha desarrollado sus capacidades cibernéticas como un componente esencial de su estrategia de guerra híbrida, utilizando tecnologías digitales para socavar infraestructuras físicas en el mundo real. Desde su incursión en el ciberespacio en la década de 2000, el régimen ha empleado una variedad de ataques cibernéticos como herramientas de

49 LEWIS, James. A. Cyber War and Ukraine. Center for Strategic and International Studies. 2022.; ROMANSKY, Sofia; HOENIG, Alisa; MEESSEN, Rick, & KRUIJVER, Kimberley. New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape. The Hague Centre for Strategic Studies and TNO, 2024.

50 SANDOVAL, Oscar. "Uso de la inteligencia de ciber amenazas como apoyo a la comprensión del adversario aplicada al conflicto Rusia-Ucrania". 2022., pp. 1-27. [en línea]. Disponible en: ArXiv abs/2205.03469

51 LEWIS, James. *Op. cit.*

52 RUBBI, Lautaro Nahuel y BARLARO, Rovati, Bruna. El planeamiento estratégico del ciberataque de Rusia a Estonia: Aproximaciones desde teoría de juegos; Universidad de las Fuerzas Armadas; Yura; 22; 4-2020; pp. 1-31

53 HANEY, Brian Seamus. Applied Artificial Intelligence in Modern Warfare and National Security Policy, Hastings Sci. & Tech. L.J., 11(1). 2020. [en línea]. Disponible en: https://repository.uchastings.edu/hastings_science_technology_law_journal/vol11/iss1/5

54 BLAS Barba, Luis Enrique. "Ciberguerra desde el Kremlin: Las capacidades cibernéticas rusas como herramienta para mantener su esfera de influencia", Universidad Pontificia Comillas – ICADE, 2020.

coerción y desestabilización. Entre 2017 y 2023, se estima que Corea del Norte robó activos virtuales por valor de 3 mil millones de dólares a través de ciberataques a plataformas de criptomonedas, proporcionando al régimen recursos vitales para sus programas nucleares.[55]

Las operaciones cibernéticas de Corea del Norte se han diseñado como una forma de guerra asimétrica, permitiendo al país compensar su inferioridad militar convencional en comparación con potencias como Estados Unidos y Corea del Sur. El uso de ciberataques permite al régimen atacar infraestructuras críticas, como redes de telecomunicaciones y sistemas bancarios, con un riesgo mínimo de represalias. En 2016, por ejemplo, hackers norcoreanos infiltraron el banco central de Bangladesh, logrando robar 81 millones de dólares a través del sistema SWIFT,[56] lo que subraya la vulnerabilidad de los sistemas financieros internacionales frente a ataques cibernéticos.[57]

Además, las capacidades de ciberataque de Corea del Norte se alinean perfectamente con su enfoque de guerra híbrida, donde se busca causar interrupciones sociales y económicas en tiempo real. Ejemplos previos incluyen ataques a sistemas de energía nuclear en Corea del Sur y a medios de comunicación, que no solo perturbaron la comunicación y los servicios, sino que también sembraron el miedo entre la población.[58] Al combinar tácticas cibernéticas con actividades convencionales, Corea del Norte ha demostrado ser un jugador formidable en el nuevo dominio de la guerra moderna, utilizando su infraestructura digital como una extensión de su estrategia militar y política.

Corea del Norte también ha utilizado sus capacidades cibernéticas para causar disrupción social y caos en los países adversarios. Infiltraciones en sistemas de infraestructura crítica, como el ataque en 2014 a Korea Hydro and Nuclear Power, donde se comprometieron diseños de plantas nucleares, ejemplifican cómo estos ataques buscan desestabilizar la confianza de los ciudadanos en sus gobiernos y amenazar la seguridad pública.[59] A medida que estas tecnologías evolucionan, los ataques cibernéticos se vuelven más sofisticados, lo que a su vez eleva el nivel de riesgo en la infraestructura de seguridad nacional de los países objetivo.

Consideraciones finales

A lo largo del artículo se ha examinado diversas tendencias y características de la guerra híbrida en el contexto contemporáneo, lo que como se ha demostrado, es a la vez un fenómeno esencialmente contemporáneo, pero también una evolución de tácticas y estrategias que combinan medios convencionales y no convencionales para alcanzar objetivos estratégicos. Esta forma de conflicto se caracteriza por la utilización simultánea de múltiples instrumentos de poder,

55 SHARMA, Abhishek. North Korea's Cyber Strategy: An Initial Analysis. Observer Research Foundation, Issue Brief N° 755. 2024.
56 El sistema SWIFT (Society for Worldwide Interbank Financial Telecommunication) es una red global de mensajería financiera que facilita transacciones seguras entre bancos e instituciones financieras en todo el mundo. SWIFT. About Us. 2024. [en línea]. Disponible en: https://www.swift.com/about-us.
57 KIM, Min-hyung. North Korea's Cyber Capabilities and Their Implications for International Security. Sustainability. 2022; 14(3):1744. [en línea]. Disponible en: https://doi.org/10.3390/su14031744
58 SHARMA, Abhishek. *Op. cit.*
59 *Ibídem*.

la ambigüedad en las acciones y la integración de actores estatales y no estatales.

Una de las principales conclusiones es que las tendencias de la guerra híbrida a menudo ocurren de manera simultánea y están interconectadas. Por ejemplo, el uso de empresas privadas como actores híbridos no solo diversifica los actores involucrados, sino que también se entrelaza con la dependencia económica y las tecnologías digitales. Las empresas tecnológicas pueden ser cooptadas para desempeñar roles en conflictos híbridos, mientras que la dependencia económica se utiliza como arma para ejercer presión política.

La digitalización y el uso de nuevas tecnologías han transformado el panorama de la guerra híbrida al tener diversos usos. Un mismo actor puede usar ciberataques dirigidos a infraestructuras críticas, como redes eléctricas y sistemas de telecomunicaciones como forma de socavar la infraestructura física de un país. Pero también, utilizar estas herramientas como medio de manipulación de la información y desinformación en plataformas digitales como forma de influir en la opinión pública y socavar la confianza en las instituciones democráticas de otros actores.

En conclusión, las tendencias de la guerra híbrida no ocurren de manera aislada, sino que se manifiestan de forma simultánea y están interconectadas. La combinación de actores diversos, el uso de tecnologías avanzadas y la explotación de la dependencia económica crean un entorno complejo que desafía las respuestas tradicionales a los conflictos. Es fundamental para los Estados contemporáneos reconocer esta interconexión y desarrollar estrategias integrales que aborden las múltiples dimensiones de la guerra híbrida para proteger su seguridad y estabilidad.

Para finalizar, el rol de las grandes empresas tecnológicas en conflictos híbridos es aún difuso y abre numerosas interrogantes sobre el futuro de la guerra híbrida. Estas empresas, que poseen vastos recursos y capacidades en términos de recopilación de datos y despliegue de tecnologías avanzadas, se encuentran en una posición única para influir en el desarrollo y la resolución de tales conflictos.

Sin embargo, la falta de regulación clara y la ambigüedad en sus responsabilidades plantean importantes dilemas éticos y de gobernanza. ¿Deben estas compañías ser actores neutrales o asumir un rol activo en la defensa de los intereses nacionales? ¿Son actores con agendas propias que disputarán la hegemonía de los Estados en el orden internacional? A medida que la tecnología se desarrolla y se entrelaza aún más con las esferas militares y políticas, es crucial reflexionar sobre estas interrogantes para asegurar un marco de actuación eficaz en conflictos híbridos.

Bibliografía

ADAMSKY, Dmitry. "Cross-Domain Coercion: The Current Russian Art of Strategy." Proliferation Papers 54. Institut Français des Relations Internationales (Ifri). Noviembre 2015, p. 23.

ADOMEIT, Hannes. Germany, the EU, and Russia: The Conflict over Nord Stream 2. Centre for European Studies (European Union Centre of Excellence [EUCE] at Carleton University). 2016. [en línea]. Disponible en: Disponible en: https://carleton.ca/ces/wp-content/uploads/Adomeit-policy-brief.pdf

BAQUÉS, Josep. "La Zona Gris: El nuevo terreno en juego". Revista "Ejércitos", Nº 12. noviembre 2019. Zaragoza., pp. 11-12.

BALLVÉ, Teo. Everyday State Formation: Territory, Decentralization, and the Narco Landgrab in Colombia. Environment and Planning D: Society and Space, 30(4), 2012, pp. 603-622. [en línea]. Disponible en: https://doi.org/10.1068/d4611

BARHAM, Elena; DALY, Sarah Z.; GEREZ, Julian E.; MARSHALL, John & POCASANGRE, Oscar. "Vaccine Diplomacy: How COVID-19 Vaccine Distribution in Latin America Increases Trust in Foreign Governments." World Politics 75, 4 (2023): pp. 826-875. [en línea]. Disponible en: https://dx.doi.org/10.1353/wp.2023.a908776.

BBC News. "Profile: Russia's new military chief Valery Gerasimov". BBC News. 9 de noviembre de 2012. [en línea]. Disponible en: https://www.bbc.com/news/world-europe-20270111

BLAS BARBA, Luis Enrique. "Ciberguerra desde el Kremlin: Las capacidades cibernéticas rusas como herramienta para mantener su esfera de influencia", Universidad Pontificia Comillas-ICADE, 2020.

BOEHM, Lasse & WILSON, Alex. "EU energy security and the war in Ukraine: From sprint to marathon". EPRS (European Parliamentary Research Service). Febrero de 2023. [en línea]. Disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739362/EPRS_BRI(2023)739362_EN.pdf

BROWN, Sierra. "Russia's Use of the Energy Weapon: How Russia Manipulates Ukraine, Georgia, and the Baltic States," Scholarly Horizons: University of Minnesota, Morris Undergraduate Journal: Vol. 6: Iss. 1, Article 1. 2019. [en línea]. Disponible en: DOI: https://doi.org/10.61366/2576-2176.1073

BUNSE, Simone & COLBURN, Forrest. "Chiquita en Colombia". Academia, Revista Latinoamericana de Administración, (43), 2009, pp. 1-12.

CAPDEVILLA, Claudia Antonella. "Guerra Híbrida: las nuevas tecnologías como instrumento de guerra". CEERI Global, Año 1. Número 2. diciembre 2022. Buenos Aires, Argentina. [en línea]. Disponible en: Disponible en: https://www.ceeriglobal.org/wp-content/uploads/2023/01/Revista-CEERI-Global-N2-1-59-75.pdf

Comisión Europea. 2016. "La Comisión Europea adopta el nuevo Paquete de Medidas sobre la Migración". [en línea]. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_16_1227.

Comunicado de la Cumbre de Varsovia. 2016. Delegación de Francia ante la OTAN. [en línea]. Disponible en: https://otan.delegfrance.org/Warsaw-Summit-Communique-2016.

Europa Press. "Rusia cambia al comandante de operaciones en Ucrania". Última Hora. 11 de enero de 2023. [en línea]. Disponible en: https://www.ultimahora.es/noticias/internacional/2023/01/11/1861653/guerra-ucrania-cambio-comandante-rusia.html

FINLAY, Lorraine & PAYNE, Christian. "The Attribution Problem and Cyber Armed Attacks," American Journal of International Law 113 (2019): p. 203, [en línea]. Disponible en: https://doi.org/10.1017/aju.2019.35.

FIOTT, Daniel. "Digitalisation and Hybrid Threats: Assessing the Vulnerabilities for European Security," Hybrid CoE Papers (The European Centre of Excellence for Countering Hybrid Threats,

April 2020), Paper 13, [en línea]. Disponible en: https://www.hybridcoe.fi/wpcontent/uploads/2022/04/20220404-Hybrid-CoE-Paper-13-Digitalization-and-hybrid-threats-WEB.pdf.

GERASIMOV, Valeri. "The Value of Science is in the Foresight: The New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," trans. by Robert Coalson, Military-Industrial Kurier, (February 2013), [en línea]. Disponible en: http://usacac.army.mil.

Gobierno de España. 2017. Estrategia de Seguridad Nacional (ESN). [en línea]. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/documents/2017-1824_estrategia_de_seguridad_nacional_esn_doble_pag.pdf.

HANEY, Brian Seamus. Applied Artificial Intelligence in Modern Warfare and National Security Policy, Hastings Sci. & Tech. L.J., 11(1). 2020. [en línea]. Disponible en: https://repository.uchastings.edu/hastings_science_technology_law_journal/vol11/iss1/5

HOFFMAN, Frank. Confict in the 21st Century: The Rise of Hybrid Wars. Virginia, Estados Unidos, Potomac Institute for Policy Studies, 2017.

JOKINEN, Janne; NORMARK Magnus and FREDHOLM, Michael. "Hybrid Threats from Non-State Actors: A Taxonomy," Hybrid CoE Research Reports (The European Centre of Excellence for Countering Hybrid Threats, June 9, 2022), Report 6, [en línea]. Disponible en: https://www.hybridcoe.fi/wpcontent/uploads/2022/06/Hybrid-Coe-Research-Report-6-WEB-EDS-20221121.pdf

KIM, Min-hyung. North Korea's Cyber Capabilities and Their Implications for International Security. Sustainability. 2022; 14(3): 1744. [en línea]. Disponible en: https://doi.org/10.3390/su14031744

KIM, Victoria. "Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack," The New York Times, September 8, 2023, [en línea]. Disponible en: https://www.nytimes.com/2023/09/08/world/europe/elonmusk-starlink-ukraine.html

KORTEWEG, Rem. Energy as a tool of foreign policy of authoritarian states, in particular Russia. Policy Department for External Relations. European Parliament. 2018. [en línea]. Disponible en: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2018)603868

LEWIS, James. A. Cyber War and Ukraine. Center for Strategic and International Studies. 2022.

LONG, Tom & URDINEZ, Francisco. Status at the margins: why Paraguay recognizes Taiwan and shuns China. Foreign Policy Analysis 17(1): 2021., pp. 1–22. [en línea]. Disponible en: doi:10.1093/fpa/oraa002

MALACALZA, Bernabé. What led to the boom? Unpacking China's development cooperation in Latin America. World Affairs 182(4): 2019, pp. 370–403. [en línea]. Disponible en: doi:10.1177/0043820019883251

MARQUARDT, Alex. "Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab." CNN, October 12, 2022.

MATANIA, Eviatar. & SOMMER, Udi. Tech titans, cyber commons and the war in Ukraine: An incipient shift in international relations. International Relations, 0(0). 2023. [en línea]. Disponible en: https://doi.org/10.1177/00471178231211500

MATTIS, James N. & HOFFMAN, Frank. Future warfare: The rise of hybrid wars. Proceedings-United States Naval Institute, 131(11). 2005., pp. 18-19.

Ministerio de Defensa de España. 2017. Concepto de Empleo de las Fuerzas Armadas Españolas. [en línea]. Disponible en: https://www.defensa.gob.es/ume/Galerias/Descargas/legislacion/CONCEPTO-DE-EMPLEO-DE-LAS-FAS-ESPANOLAS-2017.pdf

MUMFORD, Andrew. "Proxy Warfare and the Future of Conflict." The RUSI Journal 158 (2): 2013., pp. 40–46. [en línea] Disponible en: doi:10.1080/03071847.2013.787733.

MURRAY, Williamson and MANSOOR, Peter R. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge University Press, 2012.

NATO. 2024. "Hybrid Threats and Hybrid Warfare." [en línea]. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf

NIETO, Paulo Felipe y SUDARSKY, Juan Bernardo. "El caso de los pagos de Chiquita Brands a los paramilitares en Colombia durante el periodo 1997-2004: Un análisis de stakeholders". Universidad de los Andes, noviembre de 2007.

OKONTA, Ike & DOUGLAS, Oronton. Where vultures feast: Shell, human rights, and oil in the Niger Delta. San Francisco: Sierra Club Books. 2001., pp. 1-286.

OKONTA, Ike. Behind the Mask: Explaining the Emergence of MEND Militia in Nigeria's Oil-Bearing Niger Delta. Institute of International Studies, University of California, Berkeley. 2006.

RICH, Timothy S. "Status for Sale: Taiwan and the Competition for Diplomatic Recognition." Issues & Studies 45 (2009): pp. 159-188.

RODRÍGUEZ, Mario Esteban. La batalla diplomática de Beijing y Taipei en América Latina y el Caribe. Revista CIDOB d' Afers Internacionals 81: 209. 231. 2008.

ROMANSKY, Sofia; HOENIG, Alisa; MEESSEN, Rick, & KRUIJVER, Kimberley. New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape. The Hague Centre for Strategic Studies and TNO, 2024.

RUBBI, Lautaro Nahuel y BARLARO Rovati, Bruna. El planeamiento estratégico del ciberataque de Rusia a Estonia: Aproximaciones desde teoría de juegos; Universidad de las Fuerzas Armadas; Yura; 22; 4-2020; pp. 1-31.

SANDOVAL, Oscar. "Uso de la inteligencia de ciberamenazas como apoyo a la comprensión del adversario aplicada al conflicto Rusia - Ucrania". 2022., pp. 1-27. [en línea]. Disponible en: ArXiv abs/2205.03469

SATARIANO, Adam; REINHARD, Scott; METZ, Cade; FRENKEL, Sheera & KHURANA, Malika. "With Starlink, Elon Musk's Satellite Dominance Is Raising Global Alarms." The New York Times, July 28, 2023. [en línea]. Disponible en: https://www.

nytimes.com/interactive/2023/07/28/business/starlink.html.

SHARMA, Abhishek. North Korea's Cyber Strategy: An Initial Analysis. Observer Research Foundation, Issue Brief N° 755. 2024.

SITARAMAN, Ganesh & PASCAL, Alex, "The National Security Case for Public AI". Vanderbilt Policy Accelerator: Vanderbilt University. 2024. [en línea]. Disponible en: https://cdn.vanderbilt.edu/vu-URL/wp-content/uploads/sites/412/2024/09/27201409/VPA-Paper-National-Security-Case-for-AI.pdf

SWIFT. About US. 2024. [en línea]. Disponible en: https://www.swift.com/about-us.

TELIAS, Diego & URDINEZ, Francisco. China's Foreign Aid Political Drivers: Lessons from a Novel Dataset of Mask Diplomacy in Latin America during the COVID-19 Pandemic. Journal of Current Chinese Affairs, 51(1), 2022., pp. 108-136. [en línea]. Disponible en: https://doi.org/10.1177/18681026211020763

TZU, Sun y ÁLVAREZ, Ricardo. El arte de la guerra. Buenos Aires: Prometeo Libros, 2016.

VON CLAUSEWITZ, Karl. De la guerra. Santa Fe, Argentina: El Cid Editor, 2003.

WÓJTOWICZ, Anna. "EU Energy Security After Russia's Invasion of Ukraine – Substance, Strategy and Lobbying". Studia Europejskie – Studies in European Affairs 2/2024, pp. 157-171.

ZHANG, Denghua & SMITH, Graeme. "China's Foreign Aid System: Structure, Agencies, and Identities." Third World Quarterly, 38 (10), 2017., pp. 2330–46. [en línea]. Disponible en: doi:10.1080/01436597.2017.1333419.