ISSN: 1390-4299
1390-3691
No. 25

URVIO

Revista Latinoamericana de Estudios de Seguridad

Amenazas híbridas

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
FLACSO Sede Ecuador • Diciembre 2019

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2019 - No. 25

URVIO está incluida en los siguientes índices, bases de datos y catálogos:

- Emerging Sources Citation Index (ESCI). Índice del Master Journal List de Thomson Reuters.
- SciELO Ecuador. Biblioteca electrónica.
- Redalyc. Red de Revistas Científicas de América Latina y el Caribe, España y Portugal.
- ERIH PLUS, European Reference Index for the Humanities and the Social Sciences. Índice de referencias.
- JournalTOCS. Base de datos.
- Directory of Research Journals Indexing (DRJI). Directorio.
- Actualidad Iberoamericana. Índice internacional de revistas.
- CLASE, Citas Latinoamericanas en Ciencias Sociales y Humanidades. Base de datos bibliográfica.
- Directorio LATINDEX, Sistema Regional de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal.
- DIALNET, Universidad de La Rioja. Plataforma de recursos y servicios documentales.
- EBSCO. Base de datos de investigación.
- FLACSO-ANDES, Centro digital de vanguardia para la investigación en ciencias sociales - Región Andina y América Latina - FLACSO, Ecuador. Plataforma y repositorio.
- REDIB, Red Iberoamericana de Innovación y Conocimiento Científico. Plataforma.
- MIAR (Matriz de Información para el Análisis de Revistas). Base de datos.
- LatAm Studies. Estudios Latinoamericanos. Base de datos.
- Google académico. Buscador especializado en documentación académica y científica.

FLACSO
ECUADOR

RELASEDOR
Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada

URVIO, **Revista Latinoamericana de Estudios de Seguridad**
Número 25, diciembre de 2019
Quito - Ecuador

ISSN 1390-4299 (en línea) y 1390-3691

URVIO, Revista Latinoamericana de Estudios de Seguridad, es una publicación electrónica semestral de FLACSO, sede Ecuador, fundada en el año 2007. La revista constituye un espacio para la reflexión crítica, el debate, la actualización de conocimientos, la investigación y la consulta sobre temas vinculados con la seguridad, el delito organizado, la inteligencia y las políticas públicas sobre seguridad en la región.

Disponible en:
http://revistas.flacsoandes.edu.ec/index.php/URVIO
http://www.flacsoandes.org/urvio/principal.php?idtipocontenido=13

Información estadística sobre tasas de aceptación e internacionalización en Urvio #25
- Número de trabajos recibidos: 11 manuscritos.
- Número de trabajos aceptados publicados: 7.
- Índice de aceptación de manuscritos: 63,63%
- Índice de rechazo de manuscritos: 36,36%.
- Número de revisores internacionales: 22
- Número de revisores nacionales: 2
- Número total de revisores por países: 6 (Argentina, Colombia, México, Chile, España y Ecuador).
- Internacionalización de autores: 4 países (Argentina, España, Costa Rica y México).

Redes sociales

@revistaurvio
@revista_URVIO
Blog: https://revistaurvio.wordpress.com/
Academia.edu: https://flacso.academia.edu/RevistaUrvio

FLACSO
ECUADOR

RELASEDOR
Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada

El Comité Editorial de URVIO decidirá la publicación o no de los trabajos recibidos, sobre los cuales no se comprometerá a mantener correspondencia. Los artículos serán sometidos a la evaluación de expertos mediante el sistema de doble ciego. Las opiniones y comentarios expuestos en los trabajos son de responsabilidad estricta de sus autoras y autores, y no reflejan la línea de pensamiento de FLACSO, sede Ecuador. Los artículos publicados en URVIO son propiedad exclusiva de FLACSO, sede Ecuador. Se autoriza la reproducción total o parcial de los contenidos siempre que se cite como fuente a URVIO, Revista Latinoamericana de Estudios de Seguridad.

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2019 - No. 25

Tema central

Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. 8-23
Mariano Bartolomé

Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad 24-40
Juan-Manuel Aguilar-Antonio

Reconceptualizando la relación entre tecnología, instituciones y guerra 41-56
Alfredo-Leandro Ocón y Aureliano da Ponte

El componente social de la amenaza híbrida y su detección con modelos bayesianos 57-69
Ana-María Ruiz-Ruano, Jorge López-Puga y Juan-Jose Delgado-Morán

Misceláneo

Narcomenudeo y control territorial en América Latina. 71-86
Sebastián Saborío

La Guardia Nacional y la militarización de la seguridad pública en México 87-106
Gerardo Hernández y Carlos-Alfonso Romero-Arias

Estudios Globales

El tratamiento informativo de la guerra híbrida de Rusia 108-121
Javier Miguel-Gil

Política editorial. 122-140

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2019 - No. 25

Central topic

Hybrid Conflicts and Threats: Main Features, its Evolution across Time and Preponderant Forms 8-23
Mariano Bartolomé

Cyber-physical Facts: A Proposed Analysis for Cyber Threats in the National Cybersecurity Strategies 24-40
Juan-Manuel Aguilar-Antonio

Reconceptualizing the Relationship between Technology, Institutions and War 41-56
Alfredo-Leandro Ocón y Aureliano da Ponte

The Social Component of the Hybrid Threat and its Detection with Bayesian Models 57-69
Ana-María Ruiz-Ruano, Jorge López-Puga y Juan-Jose Delgado-Morán

Miscellaneous

Small Scale Drug Trafficking and Territorial Control in Latin America 71-86
Sebastián Saborío

The National Guard and the militarization of public security in Mexico 87-106
Gerardo Hernández y Carlos-Alfonso Romero-Arias

Global Studies

The Informative Treatment of the Russian Hybrid War 108-121
Javier Miguel-Gil

Política editorial. 122-140

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2019 - No. 25

Tema central

Ameaças e conflitos híbridos: características distintivas, evolução ao longo do tempo e manifestações predominantes. 8-23
Mariano Bartolomé

Fatos ciber-físicos: uma proposta de análise para ameaças cibernéticas nas Estratégias Nacionais de Segurança Cibernética 24-40
Juan-Manuel Aguilar-Antonio

Reconceituando a relação entre tecnologia, instituições e guerra 41-56
Alfredo-Leandro Ocón y Aureliano da Ponte

O componente social da ameaça híbrida e sua detecção com modelos bayesianos 57-69
Ana-María Ruiz-Ruano, Jorge López-Puga y Juan-Jose Delgado-Morán

Diversos

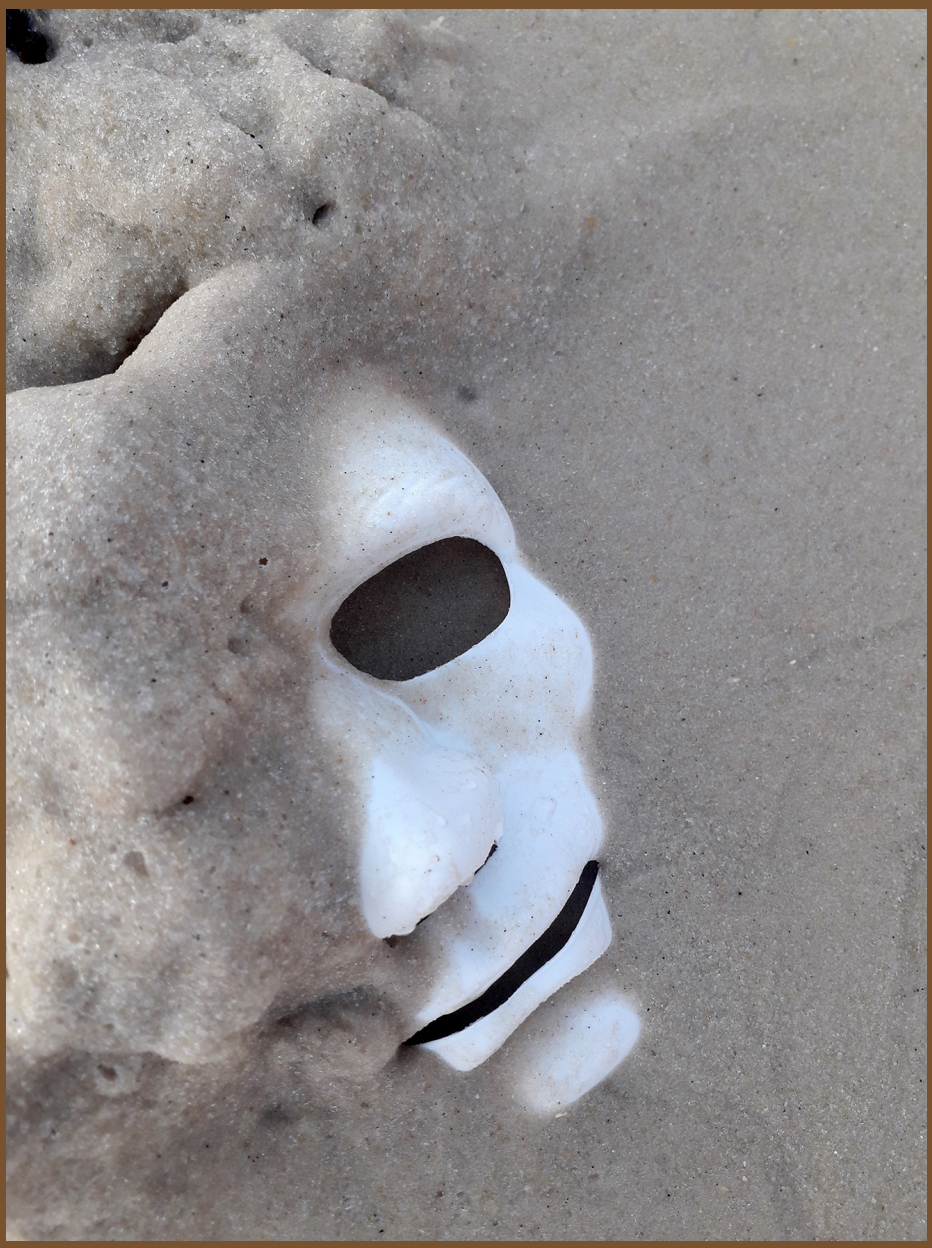
Varejo de drogas e controle territorial na América Latina 71-86
Sebastián Saborío

A Guarda Nacional e a militarização da segurança pública no México 87-106
Gerardo Hernández y Carlos-Alfonso Romero-Arias

Estudos Globais

O tratamento informativo da Guerra híbrida russa 108-121
Javier Miguel-Gil

Política editorial. 122-140



Estudios Globales

doi.org/ 10.17141/urvio.25.2019.4006

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 25, diciembre 2019-mayo 2020
pp. 108-121 • RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

El tratamiento informativo de la guerra híbrida de Rusia

The Informative Treatment of the Russian Hybrid War

Javier Miguel-Gil[1]

Recibido: 3 de junio de 2019
Aceptado: 2 de septiembre de 2019
Publicado: 2 de diciembre de 2019

Resumen

El artículo tiene como objetivo analizar el tratamiento informativo que los medios de comunicación han realizado de las campañas de desinformación rusa en un supuesto contexto de guerra híbrida. A partir de noticias de los principales medios de comunicación que informaron sobre el tema, el análisis se centra en el uso del concepto de guerra híbrida y lo compara con su concepción tradicional estratégica, para determinar si las actividades en cuestión pueden inscribirse en este tipo de conflictos.

Palabras clave: doctrina Gerasimov; guerra híbrida; medios de comunicación; propaganda; Rusia

Abstract

The objective of this paper is to analyze the treatment that the mass media have given to Russian disinformation campaigns in a supposed context of hybrid war. The exposition of news from the main mass media allows to focus the analysis on the concept of hybrid war, and to compare it with its traditional strategic conception, to determine if the activities in question can be classified into this kind of conflicts.

Key Words: Gerasimov Doctrine; hybrid warfare; mass media; propaganda; Russia

1 Universidad Complutense de Madrid, España, javier.miguel.gil@ucm.es, orcid.org/0000-0002-5141-1024

Introducción

La incorporación de las Tecnologías de la Información y Comunicación (TIC) ha comportado un cambio total en la forma en que nos relacionamos y comunicamos, pero también en la forma en que nos informamos. La expansión de lo que hoy conocemos como internet ha permitido que millones de personas en todo el mundo tengan acceso a la mayor fuente de información en la historia de la humanidad, principalmente a través de los *smartphones*, los ordenadores personales y las *tablets*.

Uno de los ámbitos en los que la propagación de internet ha tenido mayor repercusión ha sido en la comunicación, tanto en la estructura de los medios y en el alcance de su audiencia como en los propios contenidos. Los medios tradicionales han tenido que adaptar su organización a nuevos formatos y a una demanda continua de información por parte de los lectores, además de hacer frente a la aparición de nuevos medios, exclusivamente digitales. Pero esa exigencia informativa ha generado también ciertas dudas sobre la credibilidad y calidad de la información, algo realmente preocupante si tenemos en cuenta la importancia de los medios de comunicación en las sociedades democráticas. La rapidez con la que se propagan las noticias actualmente –bien sea a través de los sitios webs, de los medios de comunicación o de las redes sociales– tiene un impacto prácticamente inmediato en la opinión pública y, en muchos casos, también efímero. La necesidad de generar continuamente noticias ha comportado que estas tengan una enorme volatilidad, a la vez que ha condicionado la calidad de la información.

En ese contexto, las denuncias públicas por parte de los gobiernos occidentales sobre unas supuestas campañas de desinformación dirigidas desde el gobierno de Vladimir Putin (Boffey 2018; Faus 2018) han centrado gran parte de la atención mediática internacional. Conceptos como ciberataques, *fake news* y amenazas híbridas se han generalizado para denunciar la propagación de noticias falsas con el objetivo de desestabilizar, en procesos internos como el *Brexit* (junio de 2016), en las elecciones presidenciales estadounidenses (noviembre de 2016) y en la crisis política y social catalana en España (con su punto álgido en octubre de 2017). Según las denuncias, los intentos de injerencia se basarían en el uso de la información entendida como un elemento militar, de carácter asimétrico, en un supuesto contexto de guerra híbrida, dirigida desde la Federación de Rusia contra las democracias occidentales, a través de la denominada "doctrina Gerasimov".

Metodología

El presente análisis tiene como objetivo comparar el tratamiento periodístico que los medios han dado a las campañas de desinformación rusa y a las cuestiones híbridas con el concepto de lo híbrido desarrollado tradicionalmente desde un ámbito estratégico-militar, para determinar si los acontecimientos citados se inscriben en un contexto de guerra híbrida, tal y como señalan gran parte de los medios y analistas.

El artículo parte de la exposición de una serie de noticias relacionadas con las campañas de desinformación de origen ruso y del uso que hicieron del concepto de guerra híbrida. Debido a la gran cantidad de noticias publicadas sobre estas cuestiones, a partir del procedimiento sintético, se realizó una selec-

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 108-121
ISSN 1390-4299 (en línea) y 1390-3691

ción general de noticias de distintos medios de reconocido prestigio nacional e internacional que aportan una variedad de perspectivas como *The Guardian, The Washington Post, BBC* y *El País*. Posteriormente, y siguiendo el método descriptivo, se introduce el término guerra híbrida desde su concepción tradicional, partiendo del origen del concepto, exponiendo algunas de sus definiciones y características generales y contextualizándolo en lo que se ha popularizado como doctrina Gerasimov. Por último, a través del método comparativo, se compara el tratamiento periodístico de este tipo de conflictos con su concepción tradicional estratégica.

Contextualizando la guerra híbrida

En los últimos años, tomando como referencia temporal el referéndum que tuvo lugar en Reino Unido para abandonar la Unión Europea, en junio de 2016, y especialmente desde las elecciones presidenciales estadounidenses de noviembre de ese mismo año, los medios de comunicación han centrado gran parte de su información internacional en alertar sobre el peligro que las noticias falsas –popularizadas con el nombre de *fake news*– representan para las democracias occidentales.

En su objetivo de informar, los medios de comunicación masiva han utilizado todo tipo de conceptos, nuevos para gran parte del público, como ciberespacio, ciberataque, ciberguerra o guerra híbrida, para explicar los acontecimientos que se producían a través de lo que comúnmente denominamos internet, en los que un Estado (la Federación Rusa en este caso) utilizaría el ámbito digital para interferir en procesos internos de otro, con el objetivo de desestabilizar sus sistemas democráticos. En este novedoso y complejo contexto, ¿cómo informaron los medios de comunicación sobre los sucesos?

A pesar de que actualmente el *Brexit* se considera un ejemplo de las injerencias rusas en campaña electoral (Cohen 2018), encontramos pocas referencias en los medios que, tanto durante la campaña como en el momento posterior al referéndum, acusaron al gobierno de Vladimir Putin de querer influir en la votación del referéndum y definieron esas actividades como guerra híbrida.[2] En su mayoría, los análisis postelectorales se centraron en la incertidumbre que generaba la salida de Reino Unido de la Unión Europea, en las consecuencias económicas, políticas y sociales que podría tener, así como en el propio papel de la Unión a partir de ese momento (BBC 2016; Coy 2016).

En gran medida, no fue hasta las elecciones presidenciales estadounidenses, celebradas en noviembre de 2016, cuando los medios de comunicación señalaron directamente a Moscú de haber realizado ataques informáticos contra el Partido Demócrata y de haber orquestado campañas de desinformación para influir en el voto mediante la opinión pública. En este punto la atención se centró en el ciberespacio y en las vulnerabilidades que representa para las democracias occidentales. A pesar de eso, no fue hasta meses después cuando empezaron a surgir de forma continua informaciones sobre la posible injerencia del Kremlin en el referéndum británico, a través de la propagación de noticias falsas, así como el uso de las redes sociales (Adam y Booth 2017; The Economist 2017).

2 Las escasas referencias a Rusia se centraban en cómo la incertidumbre surgida a partir del triunfo del *Brexit* era bien vista desde el Kremlin –con alusiones al todavía reciente conflicto en Ucrania–, pero sin señalar directamente al gobierno de Putin por haber promovido una campaña de desinformación o de guerra híbrida (Baunov 2016).

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 108-121
ISSN 1390-4299 (en línea) y 1390-3691

Los hechos marcaron un antes y un después en el papel que habría jugado una potencia extranjera para tratar de influir en un proceso electoral interno. Fueron una señal de alerta para los países europeos que meses después iban a celebrar distintos procesos electorales[3] (Branford 2017). En ese contexto, el periódico *The Guardian* afirmaba en un titular que "La UE intensifica su campaña contra la propaganda rusa" (Boffey y Rankin 2017) debido al miedo que había generado la posible injerencia rusa en las elecciones estadounidenses, y a que esta pudiera extenderse a Europa. Señalaba que la Unión iba a "aumentar sus esfuerzos para contrarrestar la campaña de guerra híbrida de Rusia tras la elección de Donald Trump". La noticia hace referencia al *East Stratcom Task Force*, un organismo creado en 2015 por el Servicio Europeo de Acción Exterior de la UE –y, por lo tanto, anterior a los procesos aquí expuestos– para contrarrestar las campañas de desinformación rusas durante la crisis de Ucrania.

En ese contexto internacional de desinformación, noticias falsas, injerencias rusas en procesos electorales, ataques informáticos y supuesta guerra híbrida, España se encontraba inmersa en una importante crisis política y social debido a la convocatoria de un referéndum por el gobierno autonómico de la Generalitat de Catalunya, a primeros de octubre de 2017, que pretendía decidir mediante consulta sobre la posibilidad de independizarse del Estado español, sin el consentimiento del gobierno de España. Rápidamente se incorporaron estas actividades al lenguaje informativo. Titulares como "Ciberguerra entre los gobiernos catalán y español por el cierre de la web del referéndum" (Pueyo 2017), publicado en el periódico *El País* pocos días antes de la celebración del referéndum o "The great Catalonian cyberwar of 2017" (Caryl 2017), publicado por *The Washington Post,* apenas dos semanas después de que tuviese lugar el referéndum, utilizaron el concepto de ciberguerra de forma genérica, sin tener en cuenta su posible significado e implicaciones, por el simple hecho de que determinadas actividades se realizaron a través de la red.

El concepto de ciberguerra ha sido uno de los más utilizados desde el ámbito periodístico para hacer referencia a las actividades que tienen lugar a través de internet, pero a su vez ha generado confusión. Richard A. Clarke, Excoordinador Nacional de Seguridad, Protección de Infraestructura y Contraterrorismo de EEUU y Asesor Especial del presidente en Seguridad Cibernética, define la ciberguerra como "las acciones realizadas por un Estado-nación para penetrar en los ordenadores o en las redes de otros Estados con el propósito de causar daño o alteraciones" (Clarke y Knake 2010, 6). A excepción de los ciberataques contra el Partido Demócrata, por los cuales se tuvo acceso a datos de la campaña e información de miembros del Partido, las actividades de propaganda que tuvieron lugar en el *Brexit* y en el conflicto catalán no pueden calificarse de ciberguerra, según la definición de Clarke, ya que no habrían comportado el acceso ilegítimo a los sistemas o redes de otros Estados, con el objetivo de causar daño o alteraciones, sino que más bien serían actividades de influencia y manipulación a través de la red.

En el momento álgido de los acontecimientos de Catalunya, análisis y titulares como "Rusia se apunta a la guerra híbrida" (De Pedro 2017), "La guerra híbrida amenaza

3 Países Bajos celebró elecciones generales en marzo de 2017; Francia realizó las elecciones presidenciales entre abril y mayo de 2017 y, en el mes de junio, las legislativas; en Alemania se celebraron las elecciones federales en el mes de septiembre y Chéquia celebró elecciones legislativas en octubre de 2017.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 108-121
ISSN 1390-4299 (en línea) y 1390-3691

a España" (Pérez 2017) y directamente "Guerras Híbridas" (El País 2017) nos situaban en este tipo de guerras. En el último caso, el periódico afirma que la desinformación es

> parte de una doctrina militar que recibe el nombre de 'guerra híbrida'. Esta doctrina -elaborada en Rusia- busca debilitar a las democracias interfiriendo en sus procesos electorales y alimentando sus conflictos internos, sean ideológicos o territoriales, valiéndose para ello de instrumentos como las noticias falsas o la manipulación de las redes sociales (El País 2017).

Es conveniente señalar que, en algunos casos, los titulares hacen referencia a cuestiones relacionadas con informaciones o documentos gubernamentales en los que se utiliza este tipo de conceptos, como es el caso de los artículos de Pérez (2017) y el editorial de *El País* (2017), que aluden a la aprobación de la actual Estrategia de Seguridad Nacional española de 2017, la cual incluye las cuestiones de las amenazas híbridas y la desinformación.

Pero si analizamos las noticias –tanto las indicadas anteriormente como otras que tratan estas cuestiones– uno de los elementos que tienen en común es que no explican ni exponen mínimamente al lector algunos de los conceptos utilizados –entiéndase ciberataque, ciberguerra o guerra híbrida, por señalar algunos ejemplos–. En cambio, se limitan a afirmar que estamos en un conflicto (guerra híbrida) promovido por un actor estatal (Rusia), mediante la difusión de noticias falsas a través de internet y de las redes sociales, con el objetivo último de debilitar a los gobiernos democráticos occidentales. Por otro lado, gran parte de las noticias sobre estas actividades presentan la guerra híbrida como algo novedoso (El País 2017; Roig 2018), que forma parte de una doctrina militar de origen ruso conocida como doctrina Gerasimov, aunque hay referencias anteriores a estos hechos, principalmente centrados en el contexto de la crisis de Ucrania, en 2014 (Kendall 2014; Villarejo 2014).

Si revisamos las publicaciones académicas, el origen de las denominadas guerras híbridas habría que situarlo en un contexto anterior a los hechos aquí expuestos. Algunos de trabajos, publicados a principios de 2015 –por lo tanto, anteriores al *Brexit*, a las elecciones presidenciales de EEUU y a la crisis catalana– analizaban el concepto de guerra híbrida (García y Martínez-Valera 2015) o se cuestionaban si en aquel momento era un elemento novedoso o tan solo una vieja adaptación de viejos esquemas (Baqués 2015b, 3).

Origen y características de las guerras híbridas

Hay autores que atribuyen el origen de la expresión guerra híbrida al general retirado de la Armada estadounidense Robert Walker, en 1998 (Baqués 2015b, 8; Oguz 2017, 531), quien analizó en su trabajo final de máster el modelo híbrido de las guerras –centrándose en el Cuerpo de Marines de los Estados Unidos–. Por otro lado, hay quienes señalan que el origen habría que situarlo unos años más tarde, en 2002, cuando se utilizó el término para explicar acciones tácticas de la Primera Guerra de Chechenia, que tuvo lugar entre 1994 y 1996. Sin embargo, de manera oficial no se utilizó hasta la Estrategia Nacional de Defensa estadounidense de 2005 (Colom 2019, 8). No fue hasta la publicación en 2005 del artículo *Future Warfare: The Rise of Hybrid Warfare,* del general James N. Mattis y el te-

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 108-121
ISSN 1390-4299 (en línea) y 1390-3691

niente coronel Frank G. Hoffman, y del trabajo *Conflict in the 21st Century. The Rise of Hybrid Wars* (Hoffman 2007) cuando el concepto adquirió contenido teórico y se popularizó (Colom 2019, 8-9).

El concepto se extendió en gran medida para intentar comprender las guerras contemporáneas entre actores estatales y no estatales, en las que un actor estatal teóricamente superior en tecnología, capacidad militar o doctrinal no era capaz de doblegar a actores irregulares. Un ejemplo de ello son las guerras que llevaron a cabo los EEUU en Afganistán (inició en 2001) e Irak (inició en 2003) y la campaña que enfrentó a Israel contra Hezbollah en el verano de 2006 (Baqués 2015b, 3).

Definiciones de guerra híbrida

Una de las primeras aproximaciones define la guerra híbrida como "la que se sitúa en los intersticios entre la guerra especial y la guerra convencional" (Walker 1998, 4-5). Por su parte, Hoffman (2007, 28) amplía y precisa su naturaleza, y considera que "mezcla la letalidad del conflicto estatal con el fervor fanático y extendido de la guerra irregular". Puede ser promovida tanto por actores estatales como no estatales. Estos conflictos "incorporan una variedad de diferentes modos de hacer la guerra, incluyendo capacidades convencionales, tácticas y formaciones irregulares, actividades terroristas incluyendo violencia y coerción indiscriminada y desorden criminal" (Hoffman 2007, 29). En la práctica, ello supone la combinación de actividades convencionales e irregulares. En una línea similar, el coronel de Infantería del Ejército de Tierra español, José Luis Calvo Albero, define la guerra híbrida como "aquella en la que al menos uno de los adversarios recurre a una combinación de operaciones convencionales y guerra irregular, mezclada esta última con acciones terroristas y conexiones con el crimen organizado" (Palacios 2016b, 22).

A pesar de estas aproximaciones,[4] actualmente no hay una definición precisa del concepto, que sea ampliamente aceptada, "más allá del mínimo común denominador de la combinación de medios, procedimientos y tácticas convencionales y asimétricas" (Colom 2018, 30). Inclusive, hay quienes plantean que "no hay nada nuevo sobre el concepto de las operaciones híbridas o su utilidad en el conflicto" (Walker 1998, 5). En los conflictos de la posguerra fría, quienes se han enfrentado a Estados occidentales habrían utilizado (en distintos niveles) fuerzas convencionales, tropas irregulares, actos terroristas y crimen organizado (Baqués 2015b, 10-11).

Características de las guerras híbridas

Las noticias han presentado la guerra híbrida como un conflicto novedoso, centrándose principalmente en el elemento informativo –en la desinformación y las noticias falsas– y en su difusión por internet. Pero este tipo de conflictos supondrían, además, la combinación de otros elementos a tener en cuenta, como los actores que participan, el tipo de armamento que poseen y los escenarios en los que se desarrollan (Baqués 2015a). Algunas características de las guerras híbridas son:

4 El objetivo es presentar una aproximación general al concepto de guerra híbrida y sus características, pero no hay que obviar el debate en torno a la propia conceptualización, cuya discusión escapa del objetivo del presente artículo y su extensión. Para una ampliación del debate y distintas aproximaciones al concepto, ver: Johnson 2018; Schnaufer 2017; Wither 2016.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 108-121
ISSN 1390-4299 (en línea) y 1390-3691

- Los actores de los conflictos: entre ellos encontramos Estados, grupos guerrilleros y terroristas, así como grupos de crimen organizado o contratistas militares privados (Colom 2012, 79). Este tipo de conflictos pueden ser planteados por actores estatales o actores no estatales (Baqués 2015b, 3-7). Como se ha señalado anteriormente, los análisis de la guerra híbrida se centraron principalmente en los enfrentamientos entre actores armados no estatales –normalmente vinculados a un Estado fallido– y los Estados occidentales, como en los casos de las guerras de Afganistán, Irak y el enfrentamiento entre Hezbollah e Israel. Los grupos insurgentes desarrollarían la guerra híbrida debido a que, *a priori*, tendrían unas capacidades inferiores a los actores estatales –en personal, doctrina, armamento y tecnología– en una eventual guerra convencional. Formados principalmente por voluntarios, el objetivo consistiría en contrarrestar la superioridad del actor estatal y explotar sus vulnerabilidades.[5] Por otro lado, este tipo de conflictos también pueden plantearse por parte de actores estatales, en un eventual enfrentamiento convencional con otros actores estatales supuestamente superiores. Un caso novedoso sería el conflicto entre Ucrania y Rusia en 2014, en el que el Estado teóricamente más fuerte (Rusia) fue quien usó la guerra híbrida contra el más débil (Baqués 2015a). Baqués añade que esa decisión se basaría en evitar un enfrentamiento convencional y, a su vez, un posible choque con Estados Unidos y la OTAN, en el que Rusia sería precisamente la "parte débil".
- El tipo de armamento utilizado: las fuerzas irregulares poseen armamento más propio de los ejércitos regulares, como son tecnologías de última generación y armas pesadas, por lo que es más difícil distinguir entre las formas de guerra convencional e irregular. Baqués (2015a; 2015b, 8) hace referencia a la idea de Colin Gray del *blurring* (difuminación), en el sentido de que no hay distinción clara entre las guerras convencionales y las irregulares.
- Las tácticas empleadas: desde el uso de acciones convencionales hasta actos terroristas; el empleo de *proxies*, insurgencia, operaciones informativas o ciberoperaciones (Colom 2019, 11).
- El uso de las Tecnologías de la Información y de la Comunicación (TIC): incluye desde el control de los medios tradicionales hasta internet y las redes sociales. Ello permitiría reforzar la imagen propia o contrarrestar la del adversario, con el objetivo de llegar a los "corazones y las mentes" de las personas, lo que en buena medida sería la guerra psicológica (Baqués 2015a). De esa manera, hay una creciente importancia de la denominada guerra de la información y del uso del ciberespacio (Baqués 2015b, 12).
- Los escenarios: este tipo de conflictos se consideran esencialmente urbanos, a diferencia de las guerras de guerrillas, que se desarrollarían en la selva o las montañas. Esto genera mayores dificultades para alcanzar los objetivos militares, debido a la presencia de la población civil y a las posibles consecuencias en las infraestructuras como el transporte y la energía.
- La conexión con grupos terroristas y el crimen organizado: es habitual que los

5 Por ejemplo, alargando el conflicto. Este hecho implicaría un desgaste del Estado occidental en cuestión, debido principalmente a la creciente presión de la opinión pública. A la vez, cuanto más se alarga el conflicto, mayores son los costes económicos. Los casos de Afganistán e Irak y su impacto económico y en la opinión pública son un ejemplo.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 108-121
ISSN 1390-4299 (en línea) y 1390-3691

grupos que participan en las guerras híbridas tengan vínculos con grupos terroristas (realización de atentados terroristas) o delincuencia organizada (en el ámbito de la financiación). Esto no implica necesariamente que tengan objetivos comunes.

- La creciente importancia del elemento psicológico: hay un desprecio intencionado hacia la legalidad y el derecho internacional humanitario por parte de los actores promotores de las guerras híbridas y de los grupos criminales y terroristas vinculados. Por el contrario, las fuerzas armadas occidentales se encuentran sujetadas a reglas –*ius in bello*, las tradiciones militares o las Reglas de Enfrentamiento (ROE, por sus siglas en inglés) – (Baqués 2015b, 6). Por ello, las guerras híbridas pueden considerarse formalmente distintas a los conflictos tradicionales, en cuanto se "combatía de manera convencional y simétrica en frentes claramente definidos, con medios tecnológicamente avanzados para la época, y sometidos a los usos y costumbres de la guerra comúnmente aceptados por los contendientes" (Colom 2012, 80).
- La planificación: los promotores de este tipo de conflictos detectarían previamente los puntos débiles del adversario, en el ámbito político, ideológico, económico o demográfico, con el objetivo de alargar el conflicto, de encarecer sus costes o influir en la percepción de las sociedades y de los Estados occidentales (Baqués 2015b, 5-6).

Hay que destacar, tal y como han señalado anteriormente Hoffman (2007), Calvo Albero (Palacios 2016b, 22), Colom (2018, 30) y Baqués (2015a), que las guerras híbridas implican la combinación de elementos regulares e irregulares. Por tanto, el uso de uno de estos elementos no implica que un conflicto pueda considerarse necesariamente "híbrido". Las actividades rusas en los casos expuestos (*Brexit*, elecciones estadounidenses y conflicto catalán) han recibido el calificativo de híbrido en gran medida por el uso del ciberespacio y la combinación de ataques informáticos, propaganda y desinformación a través de las TIC, así como de operaciones informativas. Sin embargo, no se produjo en ningún caso un enfrentamiento armado en el que participaran actores estatales o no estatales.

La guerra híbrida en relación con las noticias

Según los medios de comunicación, Rusia está impulsando una guerra híbrida contra los Estados occidentales. No obstante, la clasificación anterior plantea un escenario distinto a los descritos. La novedad, de acuerdo con las noticias, reside en que un único Estado (Rusia) estaría impulsando este tipo de guerras prácticamente de forma simultánea contra varios Estados a la vez, entre los que se incluyen desde las principales potencias militares (Estados Unidos y Gran Bretaña) hasta países con un menor poder militar (como sería el caso de España).[6] Esto, mediante un proceso continuo que se alarga en el tiempo, pero en el que podemos identificar momentos álgidos de presión, por ejemplo, poco antes de los procesos electorales internos. Recurriría al potencial de las TIC, sobre todo en relación con el uso del ciberespacio, para la realización de campañas de desinformación y la distribución de noticias falsas en contextos de tensión interna de los países, explotando el potencial

6 En relación con un hipotético enfrentamiento armado entre Rusia y otro actor estatal.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 108-121
ISSN 1390-4299 (en línea) y 1390-3691

que actualmente tienen internet y las redes sociales en las sociedades occidentales. Pese al uso que Rusia ha hecho del ámbito digital, unido a las campañas de desinformación, no tiene el monopolio de estas actividades, sino que cualquier Estado –así como los actores no estatales– puede hacer uso de ellas para conseguir sus objetivos. Sin embargo, los medios de comunicación han informado que es una actividad casi exclusiva de Rusia.

Hay que tener en cuenta que una de las características fundamentales de la guerra híbrida consistiría no solo en el uso de las TIC, sino en la utilización simultánea de otros componentes señalados anteriormente (Baqués 2015a; Baqués 2015b, 12). Es decir, la combinación de los elementos regulares e irregulares a los que hacía referencia Hoffman (2007). En la supuesta guerra híbrida de Rusia contra los Estados occidentales no se produce un conflicto armado en el que participen fuerzas regulares e irregulares, se use armamento avanzado[7] o se realicen actos terroristas, por citar algunos elementos.

Una de las características que señalaban los medios de comunicación era la supuesta novedad de este tipo de conflictos y la exclusividad que tenía Rusia en el planteamiento de las guerras híbridas. Pero según lo expuesto, algunos de los principales estudios se remontan a principios del siglo XXI, en un intento de comprender y definir los conflictos contemporáneos (Walker 1998; Hoffman 2007). Algunos expertos consideran que "estas formas de actuación difícilmente pueden calificarse como novedosas o considerarse como una respuesta específica al estilo occidentalizado de combate" (Colom 2012, 80). Tampoco sería novedad la difusión de noticias falsas, un elemento utilizado a lo largo de la historia, que se habría beneficiado de las tecnologías disponibles en cada momento histórico. Sí lo sería el alcance que tiene actualmente la difusión de noticias debido a la expansión de internet.

Por otro lado, uno de los elementos característicos de las guerras híbridas es el escenario en el que se desarrollan, principalmente los núcleos urbanos. En el caso que estamos analizando, Rusia habría utilizado el ciberespacio como el escenario principal de sus actividades, lo que supone otra diferencia. Por todo ello, aunque se hayan realizado operaciones informativas o ciberoperaciones a través de internet –no solo difusión de noticias, también ataques informáticos como los realizados contra el Partido Demócrata de Estados Unidos, que permitió el acceso a las cuentas de correo electrónico– estas actividades por sí solas no permitirían definir como guerra híbrida los sucesos expuestos en las noticias.

La doctrina Gerasimov y la guerra híbrida

Si el concepto de guerra híbrida ha centrado parte del análisis, otros conceptos han sido utilizados para contextualizar estos conflictos. Las noticias apuntaban a que la guerra híbrida formaba parte de una doctrina militar rusa que se ha popularizado como doctrina Gerasimov, la cual expondría que

> ahora mismo la línea que separa a la guerra de la paz es difusa, por lo que hay que desarrollar tácticas que permitan trabajar en las sombras, condicionando procesos electorales, agitando a la población civil o hackeando objetivos en otros países (Colás 2017).

7 Baqués (2015a) considera que una de las principales características de los conflictos híbridos es el uso de armamento propio de ejércitos regulares por parte de actores irregulares.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 108-121
ISSN 1390-4299 (en línea) y 1390-3691

El origen del concepto se remonta a febrero de 2013, con la publicación del artículo "El valor de la ciencia en la anticipación" (Gerasimov 2013) del jefe del Estado Mayor de la Defensa, el general Valeri Gerasimov en la revista *Voyenno-Promyshlennyy Kuryer* (VPK, Correo Militar-Industrial). Para gran parte de los medios de comunicación y analistas occidentales, el artículo representa el documento fundacional de lo que en Occidente se conoce como la doctrina Gerasimov (Bartles 2016, 55; Palacios 2016a). "Se interpreta como una propuesta de una nueva manera rusa de guerra que combina la guerra convencional y la no convencional con aspectos de poder nacional" (Bartles 2016, 55), en la que se hace referencia a los "métodos indirectos y asimétricos", que desde Occidente se han interpretado como guerra híbrida (Bartles 2016, 59). Con los sucesos de Crimea y Ucrania, se identificaron algunos de los elementos expuestos en el documento de 2013 de Gerasimov y se propagó la idea de que exponía una nueva forma de hacer la guerra[8] (Colom 2018, 34).

> Fue entonces cuando lo híbrido traspasó la frontera del debate estratégico para convertirse en vocablo de uso común y utilizarse para definir toda la gama de actividades informativas, de desestabilización y subversión que el Kremlin podía estar realizando de forma encubierta, semiencubierta o clandestina por debajo del umbral del conflicto (Colom 2019, 9).

A pesar de la aceptación generalizada del concepto y de que representa una nueva doctrina (Gamboa 2017, 31; Campos 2018, 14), algunos analistas han cuestionado que sea una doctrina militar o que proponga una nueva manera rusa de hacer la guerra (Bartles 2016, 57,63; Palacios 2016b, 27). Estos autores precisan que Gerasimov planteaba en su artículo (dirigido principalmente a un público ruso) "su perspectiva del pasado reciente, el presente y el futuro esperado de la guerra" (Bartles 2016, 55), en gran medida a partir de lo ocurrido en la "primavera árabe" y en las "revoluciones de colores". En ellas observa un aumento de medios no militares, como elementos políticos, económicos, humanitarios, operaciones encubiertas, así como la importancia de la información (Gerasimov 2013). Por su parte, Rusia considera que el concepto de guerra híbrida es un término occidental y, por lo tanto, distinto a su sistema doctrinal (Bartles 2016, 59; Palacios 2016b, 22-23). De hecho, los rusos hacen referencia a distintos términos relacionados con la guerra híbrida, como "guerra no lineal"[9] (*nelinnearnaya voyna*), "guerra ambigua" (*neopredelonnaya voyna*) y "guerra de redes" (*setovaya voyna*) (Milosevich 2017, 2).

Tres años después, Gerasimov (2016) publicó un nuevo artículo en el que expuso algunas ideas sobre las guerras contemporáneas (de forma similar al documento anterior), pero en el que añadió las experiencias de los conflictos de Ucrania y Siria. Gerasimov identifica los métodos híbridos en las revoluciones de colores y afirma que estos movimientos son, de hecho, golpes de Estado promovidos por Occidente (Palacios 2016a; Gerasimov 2016). A diferencia del artículo de 2013, este documento hace referencia de forma abierta a las guerras híbridas y a los métodos híbridos, pero de forma distinta a Occidente.

8 Hasta el inicio del conflicto en Ucrania, en 2014, las referencias a los conflictos híbridos no se relacionaban de manera específica con Rusia (Palacios 2016b, 23).

9 Este término tampoco se encuentra en la Doctrina Militar 2014, pero sí lo utilizarían Gerasimov y asesores del presidente Vladimir Putin (Milosevich 2015, 5).

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 108-121
ISSN 1390-4299 (en línea) y 1390-3691

Como se ha señalado anteriormente, la guerra híbrida combinaría métodos convencionales e irregulares –en los que encontraríamos vínculos con el crimen organizado o grupos terroristas–, mientras que, según Palacios (2016a), Gerasimov considera que

> en los conflictos contemporáneos es cada vez más frecuente que se dé prioridad a un uso conjunto de medidas de carácter no militar, políticas, económicas, informativas y de otro tipo, que se ponen en práctica con el sostén de la fuerza militar. Son los llamados métodos híbridos.

En la práctica, esto supondría una percepción más limitada de las acciones híbridas que la que tiene Occidente. A pesar de esa diferencia, el autor sostiene que la combinación de actividades tradicionales e híbridas es una característica de los conflictos armados contemporáneos, en los que señala al elemento informativo como el principal de los métodos híbridos. Esto debido a que

> la falsificación de los acontecimientos, la limitación de la actividad de los medios de información, se convierten en uno de los métodos asimétricos más eficaces para la conducción de las guerras. Su efecto puede ser comparable a los resultados de un uso masivo de tropas (Palacios 2016a).

En definitiva, Gerasimov hace referencia a la guerra y los métodos híbridos porque considera que Rusia puede tener que enfrentarse a este tipo de guerras y, por ello, debe conocerlas y adaptarse a ellas (Palacios 2016b, 26-27). Además, hay que tener en cuenta que Gerasimov lo plantea en un escenario de guerra armada, mientras que las campañas de desinformación y noticias falsas desde Occidente se realizarían en un contexto de tensión y confrontación política y social, pero en ausencia de conflicto armado. Por último –y no por ello menos importante–, Mark Galeotti (2018), el analista que acuñó el término doctrina Gerasimov, no solo ha negado la existencia de esa supuesta doctrina, sino que además señala que el artículo de Gerasimov pretendía resolver cómo luchar contra las acciones no convencionales, no promoverlas.

Conclusiones

Es habitual encontrar noticias relacionadas con las campañas de desinformación de origen ruso que afirman que estas se inscriben en un contexto de guerra híbrida contra Occidente. El principal problema de las informaciones periodísticas aquí expuestas reside en que, en su mayoría, los autores no exponen ni siquiera una breve aproximación a los conceptos utilizados, su significado e implicaciones –como pueden ser desinformación, *fake news*, ciberguerra o guerra híbrida–. En ocasiones, ello conduce a la utilización de algunos de estos conceptos como sinónimos. Posiblemente, una de las razones de la confusión es la mezcla entre el uso de conceptos recientes –en este caso, aquellos relacionados con el ciberespacio– con otros que se ubican tradicionalmente en un ámbito militar y académico, en un intento de querer informar sobre los cambios que se están produciendo en el escenario internacional. Pero también podría deberse en parte a la espiral en la que los medios de comunicación han entrado, empujados por una demanda constante de información por parte de los ciudadanos, al querer informar prácticamente al minuto sobre las últimas noticias, lo cual implica apostar por la cantidad antes que por la calidad.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 108-121
ISSN 1390-4299 (en línea) y 1390-3691

Sin duda, el uso del ciberespacio y de la información por parte de Rusia han sido el eje central de las noticias relacionadas con la guerra híbrida. Pero si bien es cierto que ese país ha fomentado el uso de las operaciones de información y ha sabido aprovechar el potencial del ámbito digital a favor de sus intereses, también lo es que el desarrollo de campañas de desinformación y el uso de las TIC no pueden identificarse exclusivamente con la guerra híbrida. Una de las características de los conflictos híbridos consiste en la combinación de distintos elementos convencionales y asimétricos, pero las noticias se han centrado casi exclusivamente en el elemento digital, a través del cual se han desarrollado las campañas de desinformación, las noticias falsas y el uso masivo de las redes sociales. A pesar de que pueden formar parte de los conflictos híbridos y de que en los últimos años el elemento ciber está adquiriendo una enorme importancia en los conflictos, no podemos señalar que estas actividades sean *la* guerra híbrida.

Difícilmente un único Estado podría desarrollar de forma simultánea guerras de este tipo –si tenemos en cuenta los elementos militares y no militares– contra todos los Estados occidentales que han denunciado estas actividades, desde EEUU hasta Alemania, Francia, Reino Unido y España. Por otro lado, la guerra híbrida no es en ningún caso una estrategia exclusiva de Rusia –ni forma parte de una doctrina militar rusa– sino que puede ser desarrollada por otros actores estatales que tengan la voluntad y los recursos necesarios, así como por actores no estatales. Nada permite determinar la exclusividad rusa.

Por lo tanto, si concluimos que los acontecimientos que tuvieron lugar en el *Brexit*, en las elecciones estadounidenses y en el conflicto catalán no pueden calificarse como guerra híbrida, un marco de análisis para comprender las novedades que comporta el ciberespacio y su impacto en las relaciones internacionales en estos escenarios podría desarrollarse desde el concepto de la *gray zone* o zona gris. El concepto define aquellas actividades bajo el umbral del conflicto, que se realizan en tiempos de paz, a diferencia de la guerra híbrida, y que incluyen ataques informáticos o campañas de desinformación y propaganda que tendrían como característica común la dificultad de determinar su atribución. Ese concepto permitiría, por lo tanto, un análisis de las actividades que no se califican específicamente como de guerra, pero que podrían llegar a ser tan decisivas como un conflicto militar.

El análisis presentado en el artículo se ha centrado en la importancia de conceptualizar y de contextualizar los hechos de los que se informa. Es evidente que el ejercicio del periodismo difiere del ámbito académico, pero también es cierto que las noticias deben transmitir el mayor rigor posible y exponer al lector lo que sucede en su contexto concreto, intentando utilizar conceptos adecuados en cada caso. Todavía nos encontramos en una fase temprana del análisis de las capacidades que tiene el ciberespacio, y reducirlo únicamente al uso que puede hacer un único Estado para la difusión de campañas de propaganda supone no comprender su potencial en la relaciones internacionales.

Bibliografía

Adam, Karla y William Booth. 2017. "Rising Alarm in Britain over Russian Meddling In Brexit Vote". *The Washington Post*, 17 de noviembre. https://wapo.st/2Ordyoz

Baqués, Josep. 2015a. "El papel de Rusia en el conflicto de Ucrania: ¿La guerra híbrida de

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 108-121
ISSN 1390-4299 (en línea) y 1390-3691

las grandes potencias?". *Revista de Estudios de Seguridad Internacional* 1 (1): 41-60. dx.doi.org/10.18847/1.1.3

Baqués, Josep. 2015b. "Las guerras híbridas: un balance provisional". *Instituto Español de Estudios Estratégicos*, Documento de Trabajo. http://bit.ly/2XZAEFY

Bartles, Charles K. 2016. "Cómo comprender el artículo de Gerasimov". *Military Review,* marzo-abril. http://bit.ly/2OyFpTY

Baunov, Alexander. 2016. "A Multipolar Europe: Why Russia likes Brexit". *Carnegie Moscow Center*, 28 de junio.

BBC. 2016. "Brexit: What happens now?". 29 de junio, https://www.bbc.com/news/uk-politics-eu-referendum-36420148

Boffey, Daniel. 2018. "EU raises funds to fight 'disinformation war' with Russia". *The Guardian*, 5 de diciembre. http://bit.ly/33ASH6x

Boffey, Daniel, y Jennifer Rankin. 2017. "EU escalates its campaign against Russian propaganda." *The Guardian*, 23 de enero. http://bit.ly/2rzPpDA

Branford, Becky. 2017. "Information warfare: Is Russia really interfering in European states?". *BBC News*, 31 de marzo. https://www.bbc.com/news/world-europe-39401637

Campos, Miguel. 2018. "El arte operacional ruso: de Tukhachevsky a la actual 'Doctrina Gerasimov'". *Instituto Español de Estudios Estratégicos*, Documento de Opinión. http://bit.ly/34wluuo

Caryl, Christian. 2017. "The great Catalonian cyberwar of 2017". *The Washington Post*, 18 de octubre. https://www.washingtonpost.com/news/democracy-post/wp/2017/10/18/the-great-catalonian-cyberwar-of-2017/

Clarke, Richard A., y Robert K. Knake. 2010. *Cyber War: the next threat to national security and what to do about it*. EEUU: HarperCollins Publishers.

Cohen, Nick. "Why isn't there greater outrage about Russia's involvement in Brexit?". *The Guardian*, 17 de junio. https://www.theguardian.com/commentisfree/2018/jun/17/why-isnt-there-greater-outrage-about-russian-involvement-in-brexit

Colás, Xavier. 2017. "La ciberguerra, amenaza estrella en 2017". *El Mundo*, 6 de enero. http://bit.ly/2pZL0sW

Colom, Guillem. 2012. "Vigencia y limitaciones de la guerra híbrida". *Revista Científica General José María Córdova* 1 (10), junio: 77-90. doi.org/10.21830/19006586.228

Colom, Guillem. 2018. "La Doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo". *Revista Ejército* 933, diciembre. https://www.ugr.es/~gesi/Doctrina-Gerasimov.pdf

Colom, Guillem. 2019. "La amenaza híbrida: mitos, leyendas y realidades". *Instituto Español de Estudios Estratégicos*, Documento de Trabajo. http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO24_2019GUICOL-hibrida.pdf

Coy, Peter. 2016. "After Brexit, here's what's next for Europe". *Bloomberg*, 30 de junio. https://www.bloomberg.com/news/features/2016-06-30/after-brexit-here-s-what-s-next-for-europe

De Pedro, Nicolás. 2017. "Rusia se apunta a la guerra híbrida". *El País*, 19 de noviembre. https://elpais.com/elpais/2017/11/18/opinion/1511025644_093966.html

El País. 2017. "Guerras Híbridas". 4 de diciembre. https://elpais.com/elpais/2017/12/03/opinion/1512325245_721922.html

Faus, Joan. 2018. "Estados Unidos acusa a Rusia de tratar de interferir en la campaña de las legistlativas". *El País*, 3 de agosto. https://elpais.com/internacional/2018/08/02/estados_unidos/1533235587_731224.html

Gamboa, Juan A. 2017. "Amenaza Híbrida, ¿un concepto doctrinal?". *Revista Ejército* 921, diciembre: 26-43. http://www.ejercito.mde.es/Galerias/multimedia/revista-ejercito/2017/921//accesible/Revista_Ejercito_Accesible.pdf

García, Miguel, y Gabriel Martínez-Valera. 2015. "La guerra híbrida: nociones prelimi-

nares y su repercusión en el planeamiento de los países y organizaciones occidentales". *Instituto Español de Estudios Estratégicos*, Documento de Trabajo. http://bit.ly/34A06nY

Galeotti, Mark. 2018. "I'm sorry for creating the 'Gerasimov Doctrine'". *Foreign Policy*, marzo. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

Gerasimov, Valeri. 2013. "Ценность науки в предвидении". *VPK* 476 8, marzo. https://vpk-news.ru/articles/14632

Gerasimov, Valeri. 2016. "По опыту Сирии". *VPK* 624 9, marzo. https://vpk-news.ru/articles/29579

Hoffman, Frank G. 2007. *Conflict in the 21st Century. The Rise of Hybrid Wars*. Virginia: Potomac Institute for Policy Studies. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Johnson, Robert. 2018. "Hybrid War and Its Countermeasures: A Critique of the Literature". *Small Wars & Insurgencies* 1 (29): 141-163.

Kendall, Bridget. 2014. "Qué es la nueva 'guerra híbrida' entre Rusia y Occidente". *BBC Mundo*, 7 de noviembre. https://www.bbc.com/mundo/noticias/2014/11/141106_guerra_hibrida_rusia_occidente_jgc

Milosevich, Mira. 2015. "¿Por qué Rusia es una amenaza existencial para Europa?". *Real Instituto Elcano* 35/2015, julio. http://bit.ly/2R0otau

Milosevich, Mira. 2017. "El poder de la influencia rusa: la desinformación". *Real Instituto Elcano*, ARI 7/2017, enero. http://bit.ly/37LSAZk

Palacios, José Miguel. 2016a. "La doctrina Gerasimov: segunda entrega". *GESI*, Análisis 7/2016 (abril). http://bit.ly/2qXviiC

Palacios, José Miguel. 2016b. "Rusia: guerra híbrida y conflictos asimétricos". *Revista Ejército* 904, julio-agosto: 22-27. http://bit.ly/2L8hmZX

Pérez, Paula. 2017. "La guerra híbrida amenaza a España". *Estrella Digital*, 1 de diciembre. http://bit.ly/34A0AdM

Pueyo, Jordi. 2017. "Ciberguerra entre los gobiernos catalán y español por el cierre de la web del referéndum". *El País*, 14 de septiembre. https://elpais.com/ccaa/2017/09/14/catalunya/1505390726_024743.html

Roig, Clara. 2018. "Las guerras de la era de la desinformación". *La Vanguardia*, 29 de abril. http://bit.ly/34BIvfq

Schnaufer, Tad A. 2017. "Redefining Hybrid Warfare: Russia's Non-linear War against the West". *Journal of Strategic Security* 1 (10): 17-31.

The Economist. 2017. "Russian Twitter trolls meddled in the Brexit vote. Did they swing it?". 23 de noviembre. https://econ.st/2R0gz0Z

Villarejo, Esteban. 2014. "La nueva guerra híbrida". *ABC Blogs, Por Tierra, Mar y Aire*, 29 de octubre. https://abcblogs.abc.es/tierra-mar-aire/otan/nuevaguerra-hibrida.html

Walker, Robert G. 1998. "Spec Fi: The United States Marine Corps and Special Operations". Tesis de maestría, Naval Postgraduate School. https://apps.dtic.mil/dtic/tr/fulltext/u2/a359694.pdf

Wither, James K. 2016. "Making Sens of Hybrid Warfare". *Connections: The Quarterly Journal* 2 (15): 73-87.