
# LA GUERRA NO LINEAL CONTRA OCCIDENTE A TRAVÉS DE UN ESTUDIO DE CASO DE LA INJERENCIA RUSA EN EL CONFLICTO INDEPENDENTISTA CATALÁN

**ICADE**
**Facultad de Derecho**
**Trabajo Final de Máster**

MÁSTER EN ASUNTOS INTERNACIONALES:
ECONOMÍA, POLÍTICA Y DERECHO
Curso 2020-2021

Autor: Victoria Krah Ripoll
Director: Dr. Javier Gil Pérez

Madrid, Junio 2021

## RESUMEN

La propaganda, la desinformación y el espionaje han existido siempre – lo que ha cambiado es el plano y su intensidad. Muchos Estados han incorporado estos tres conceptos dentro de una estrategia mayor, popularizada como “guerra híbrida” o sus múltiples derivados. Entre estos Estados, Rusia es el que ha destacado en la última década en lo que se refiere a un empleo pronunciado de operaciones de información en el ámbito de las Relaciones Internacionales. El presente TFM pretende exponer y analizar de qué manera Rusia hace uso de las OI con un fin predominantemente ideológico y cómo se inscribe la injerencia rusa en la crisis independentista catalana en una supuesta estrategia de “desestabilización” de Occidente. Esto se lleva a cabo a través de un estudio de caso de la injerencia rusa en conflicto catalán, dimensión más manejable de estudio, identificando las variables y formas de la injerencia. Los resultados facilitan la compresión de la dimensión de tales injerencias en el plano internacional.



***PALABRAS CLAVE*:** Rusia, Occidente, Cataluña, injerencia rusa, guerra híbrida, guerra no lineal, amenaza híbrida, conflicto híbrido, ciberoperaciones, operaciones de información



## ABSTRACT

Propaganda, disinformation and espionage have always existed - what has changed is the plan and its intensity. Many states have incorporated these three concepts into a larger strategy, popularized as "hybrid warfare" or its many derivatives. Among these states, Russia is the one that has stood out in the last decade in terms of a pronounced employment of information operations (IO) in the field of International Relations (IR). This TFM aims to expose and analyze how Russia makes use of IOs for a predominantly ideological purpose and how Russian interference in the Catalan independence crisis fits into an alleged strategy of "destabilization" of the West. This is done through a case study of Russian interference in the Catalan conflict, a more manageable dimension of study, identifying the variables and forms of interference. The results facilitate the understanding of the dimension of such interference at the international level.



***KEYWORDS:*** Russia, the West, Catalonia, Russian interference, hybrid warfare, nonlinear warfare, hybrid threat, hybrid conflict, cyber operations, information operations

## ÍNDICE

**CAPÍTULO I: INTRODUCCIÓN ..... 6**

I. OBJETO ..... 9
II. OBJETIVOS ..... 9
III. ESTRUCTURA ..... 10
IV. HIPÓTESIS ..... 11
V. METODOLOGÍA ..... 11
VI. FUENTES ..... 13

**CAPÍTULO II: MARCO TEÓRICO Y ESTADO DE LA CUESTIÓN ..... 15**

I. MARCO TEÓRICO ..... 15
*i. Teoría de referencia en el marco de las RRII ..... 15*
*ii. Terminología y conceptualización ..... 16*
II. ESTADO DE LA CUESTIÓN ..... 22
*i. Época soviética ..... 22*
*ii. Actualidad ..... 23*

**CAPÍTULO III: CONTEXTUALIZACIÓN RUSIA ..... 29**

**CAPÍTULO IV: ESTUDIO DE CASO ..... 33**

I. MEDIOS DE COMUNICACIÓN ESTATALES ..... 34
II. DIFUSIÓN DE INFORMACIÓN ADVERSA A TRAVES DE CIBEROPERACIONES Y OPERARIOS ..... 36
III. DIFUSIÓN DE CONTENIDOS E INFLUENCIA POLÍTICA AUTOMATIZADA A TRAVÉS DE RRSS ..... 38
IV. PRE 1-O ..... 40
*i. Medios de comunicación estatales ..... 40*
*ii. Difusión de información adversa a través de ciberoperaciones y operarios ..... 40*
*iii. Difusión de contenidos e influencia política automatizada a través de RRSS ..... 41*
V. DURANTE 1-O ..... 42
*i. Medios de comunicación estatales ..... 42*
*ii. Difusión de información adversa a través de ciberoperaciones y operarios ..... 44*
*iii. Difusión de contenidos e influencia política automatizada a través de RRSS ..... 46*
VI. POST 1-O ..... 48
*i. Medios de comunicación estatales ..... 48*
*ii. Difusión de información adversa a través de ciberoperaciones y operarios ..... 50*
*iii. Difusión de contenidos e influencia política automatizada a través de RRSS ..... 51*

**CAPÍTULO V: CONCLUSIONES ..... 55**

I. INJERENCIA EN CATALUÑA COMO AMENAZA HÍBRIDA ..... 55
II. INJERENCIA EN OCCIDENTE COMO GUERRA NO LINEAL ..... 56
III. PERSPECTIVA Y RECOMENDACIONES ..... 57

**REFERENCIAS** ..... 60

## ÍNDICE DE ABREVIATURAS

**OI:** Operaciones de Información

**RRII:** Relaciones Internacionales

**UE:** Unión Europea

**PIB:** Producto Interior Bruto

**EE.UU.:** Estados Unidos

**URSS:** Unión de Repúblicas Socialistas Soviéticas

**CNN:** Centro Criptológico Nacional

**CNI:** Centro Nacional de Inteligencia

**OTSC:** Organización del Tratado de Seguridad Colectiva

**OTAN:** Organización del Tratado del Atlántico Norte

**CESEDEN:** Centro Superior de Estudios de la Defensa Nacional

**CNA:** Centro de Análisis Naval americano

**RBN:** Russian Business Network

**NIC:** National Intelligence Council

**IRA:** Internet Reserach Agency

**RRSS:** Redes sociales

**TIC:** Tecnologías de la Información y la Comunicación

**IIS:** Seguridad de la Información Internacional

**EEAS:** Servicio Europea de Acción Exterior

**SEPE:** Servicio Público de Empleo Estatal

**CIA:** Central Intelligence Agency

**FBI:** Federal Bureau of Investigation

**NSA:** Agencia de Seguridad Nacional, agencia de inteligencia de los Estados Unidos

**KGB:** Comité para la Seguridad del Estado, servicio secreto de la Unión Soviética

## ÍNDICE DE FIGURAS

Figura 1: *Conceptualización de las estrategias de injerencia rusa políticamente motivada en relación con las respectivas áreas geográficas de actuación* ……..p.18

Figura 2: *Mapa de Europa dividida*……..……...…..p.41

Figura 3: *Modelo de amenazas híbridas: Aplicación al caso de Cataluña*……..……p.49

# CAPÍTULO I: INTRODUCCIÓN

Actualmente es de conocimiento general que el mundo desarrollado está viviendo el periodo de paz más prolongado que el hombre ha conocido desde la Pax Romana. En particular, la Unión Europea (UE) ha logrado mantener la paz en sus fronteras durante 75 años. La creación del tribunal de la Haya, institución concebida para arbitrar posibles conflictos, presenta otro símbolo moderno para el mantenimiento de la paz.

Hablar de paz es adecuado si se concibe esta misma como la ausencia de enfrentamiento armado internacional, según la corriente minimalista (Galtung, 1996)[1]. No obstante, en el panorama actual, las amenazas se han multiplicado, ya que el "equilibrio geopolítico" es mucho mas difícil de sostener y, a su vez, se aumenta la inestabilidad (Martín, 2020). En la actualidad, las aspiraciones- fructuosas o no- de una potencia regional, como las de la Federación Rusa ('Rusia'), a un resurgimiento como potencia mundial constituyen una fuente de tensión a escala global.

A su vez, el propio concepto de guerra también ha cambiado en gran medida en los últimos tiempos: La definición de guerra es ahora mucho más fluida, tal como apunta Dan Smith, secretario de la ONG *International Alert* (Smith, 2011).

En los últimos años, el patrón de guerra que ha cobrado un especial protagonismo es el de la "guerra híbrida", que combina el uso de la fuerza convencional, militar, con otros elementos como pueden ser los ciberataques, la manipulación de la información ('desinformación') a través de internet y de redes sociales, entre otros (LISA Institute, 2019).

No obstante, ni el tipo de guerra ni sus medios son nuevos: El elemento clave, lo que ahora se ha popularizado como *fake news* o desinformación, ha existido durante toda la historia de la humanidad. Tal ha sido su impacto que, no solo han manipulado en una cantidad de ocasiones a lo largo de la historia la opinión pública- véase la campaña de calumnias de Marco Antonio 44AD (Posetti & Matthews, 2018)- , sino también ha llegado a desatar la ilustre guerra

[1] Galtung,diferencia en su teoría de conflictos entre 'paz positiva' y 'paz negativa', definiendo esta última como "la ausencia de un enfrentamiento violento y el mecanismo para alcanzar esa meta es la solución de los conflictos existentes."

hispano-estadounidense de 1898[2], identificada por historiadores como la primera guerra impulsada por la prensa.

Sin embargo, si antes los *fake news* eran mayormente un medio para llegar a su fin – el de desatar una guerra tradicional, es decir, de carácter militar- ahora se pueden considerar un fin en si mismo, al tener una fuerte motivación ideológica con capacidad de influir en la opinión publica de las democracias actuales (López Jiménez, 2019). Asimismo, el nuevo escenario bélico que presenta el ciberespacio– que Rusia denomina "espacio informacional" (Thomas, 2001) – ha multiplicado los riesgos de la distribución de desinformación- en especial en cara a las democracias occidentales.

La narrativa es amplia: expertos y analistas internacionales han estudiado por un lado el concepto de guerra híbrida desde una perspectiva político-social hasta la estratégico-militar y han demostrado, por otro lado, de manera empírica las injerencias rusas en Occidente, sea mediante intervenciones en elecciones como en el Reino Unido, los Países Bajos o en EE. UU., o bien mediante ciberataques, *fake news* o desinformación.

En lo que concierne nuestro objeto de estudio, Cataluña, hubo un incremento del 2.000% de la actividad relacionada con la comunidad autónoma en Rusia por parte de las RRSS pro-rusas, según un artículo publicado por el director adjunto de *El País* en el mismo periódico (Alandete, 2017). Este hecho también ha sido señalado por el Centro Criptológico Nacional (CNN), dependiente del Centro Nacional de Inteligencia (CNI), en una nota a pie de página de un documento del 2018 titulado "Ciberamenazas y Tendencias", sugiriendo que "(p)arece demostrada la presencia de activistas patrocinados por instituciones rusas en la expresión mediática del conflicto derivado de la situación creada en Cataluña durante 2017 (…)" (CNN, 2018, pág. 10), confirmando por primera vez una injerencia rusa sin antecedentes en territorio español.

Más recientemente, en un artículo publicado por El Mundo en febrero de 2021 (Colás, 2021) – en donde se relata cómo el ministro de exteriores ruso, Sergey Lavrov, intentó dibujar un paralelismo entre las denuncias europeas sobre la situación de Navalny y el juicio a los independentistas en España – se puede corroborar la vigencia del asunto hasta en la actualidad,

[2] Cuando el Reino de España se enfrentaba a los insurrectos cubanos en 1898, bajo el mando del magnate estadounidense de la prensa amarilla William Randolph Hearst, se publicaron el periódico New York Jornal artículos sensacionalistas y material grafico conscientemente inventado, que finalmente desató la guerra.

aunque han habido numerosos artículos de prensa que han cubierto la materia a lo largo del tiempo.

Sin embargo, a mi saber, no ha habido ningún estudio académico actualizado y expresamente enfocado al caso de la injerencia rusa en el conflicto catalán, si bien caben destacar dos documentos de investigación de Mira Milosevich-Juaristi: uno titulado *El poder de la influencia rusa: la desinformación* y otro *La "combinación", instrumento de la guerra de la información de Rusia en Cataluña*. Ambos fueron publicados en el Real Instituto Elcano en 2017 y también se les hará referencia a lo largo de este trabajo.

El creciente interés que, ante una "crisis del multilateralismo" lleva a algunos analistas incluso a hablar de una "nueva Guerra Fría" (quédese al margen si con razón o no), convierte al tema objeto de este estudio de caso en una cuestión de enorme vigencia. La relevancia de este trabajo, por ende, abarca la actualidad y la realidad de un tema estratego-político y político-social, así como materia de seguridad nacional e internacional. De este modo, este trabajo espera aportar una reflexión y evaluación crítica a un tema de relevancia actual en el terreno de las RRII.

El valor teórico añadido de este trabajo se refleja en la recopilación y aclaración de conceptos teóricos como la guerra no lineal, el conflicto híbrido, la amenaza híbrida, la desinformación y los *fake news*, actualizándolos a las circunstancias actuales en el marco temático acordado. Del mismo modo, el presente trabajo pretende crear modelos conceptuales nuevos que relacionan diferentes variables, exponiendo una directa relación entre la injerencia rusa en la comunidad autónoma de Cataluña y la estrategia de una guerra no lineal contra Occidente.

Por ultimo, a nivel personal, existe una doble motivación. Por un lado, la realización de un documento de investigación en el CESEDEN sobre el poder y las personalidades en Rusia– proyecto en el cual colaboré por mi ya anteriormente existente interés en las cuestiones geopolíticas rusas.

Por otro lado, siendo parcialmente de origen catalán, he seguido – aunque desde el extranjero – la cobertura y el tratamiento informativo respecto a la crisis política y social en Cataluña con especial interés y atención.

## I. OBJETO

Se pueden diferenciar dos objetos estatales de estudio, aunque cada uno de ellos abordado desde dos aspectos ligeramente diferentes.

En un primer circulo concéntrico, en cierta medida, Rusia y España como representantes de sus respectivos bloques ideológicos, España siendo miembro de la UE y con ello necesariamente también de la OTAN, y por ende del "bloque occidental", y Rusia como heredera de la URSS y exintegrante del antiguo Pacto de Varsovia, cuyo vacío es parcialmente sustituido por otras alianzas, tales como la Organización del Tratado de Seguridad Colectiva (OTSC).

En un segundo circulo concéntrico, Rusia y España como entes soberanos con propios intereses estratégicos y geopolíticos, naturales en países con relevancia en el escenario internacional.

El objeto del trabajo gira por tanto en la supuesta injerencia de Rusia en la comunidad autónoma española de Cataluña, enmarcado en un espacio temporal de 2013, con su punto álgido en el referéndum ilegal de independencia el 1 de octubre de 2017 ('1-O'), hasta la actualidad, así como con vistas al futuro.

## II. OBJETIVOS

En primer plano, el presente análisis tiene como objetivo principal analizar los motivos de la injerencia de Rusia en Cataluña, dentro de su supuesta guerra no lineal, como método militar asimétrico, que Rusia libra en Occidente- una injerencia aparentemente de naturaleza contradictoria a su propia política interna y su posición respecto a movimientos secesionistas dentro de la propia Rusia.

En segundo plano, y con el fin de complementar el principal objetivo, está el de exponer y entender los conceptos, como la concepción rusa de la guerra no lineal, amenaza híbrida y operaciones de información (OI) para arrojar algo de luz a este fenómeno, mucho más amplio y complejo que la simple desinformación o noticias falsas.
Una vez aclarados tales conceptos, se va a analizar el grado de injerencia rusa en Cataluña, las acciones y estrategias allí implementadas por parte de Rusia y evaluar si se puede considerar como parte de una denominada guerra no lineal.

## III. ESTRUCTURA

Partiendo de las premisas expuestas, el trabajo está estructurado en cinco capítulos: introducción, marco teórico y estado de la cuestión, contextualización de Rusia, estudio de caso y conclusiones.

En el apartado referente al marco teórico, se va a proceder por un lado a delimitar el marco de referencia teórico y, por otro lado, a aclarar conceptos y los diferentes elementos definitorios de la guerra no lineal para partir de una base preestablecida. El estado de la cuestión, a su vez, pretende dar una visión de los antecedentes históricos y contemporáneos de la actividad rusa en materia de OI.
Seguidamente, se dedica un capítulo a la contextualización de Rusia, para luego abordar el estudio de caso, el cual se divide en seis bloques: en los primeros tres, se presentarán cada una de las tres líneas de actuación identificadas a la hora de llevar a cabo las OI rusas.
Los otros tres bloques se dedicarán después a los tres respectivos marcos temporales elegidos: Pre 1-O; durante 1-O; post 1-O. A su vez, cada uno de estos bloques se subdivide en secciones referentes a cada una de las líneas de actuación anteriormente definidas.

El trabajo cierra con unas conclusiones al hilo de los apartados del análisis que preceden, donde se presenta una evaluación crítica de lo analizado, así como recomendaciones y una breve reflexión sobre la posible sofisticación de los métodos usados por Rusia en este ámbito.

## IV. HIPÓTESIS

El presente trabajo parte de la siguiente pregunta inicial: ¿En qué medida constituye Cataluña el talón de Aquiles para el discurso antioccidental, dentro del marco de estrategia de "guerra híbrida" o "guerra no lineal" perseguida por Rusia?

Ante esta pregunta, se presenta la hipótesis principal: la existencia de una estrategia antioccidental por Rusia, reflejada en la denominada "guerra no lineal", con el fin de desestabilizar Europa (como pars pro toto para Occidente), a través de una injerencia en el conflicto independentista catalán. Dicha hipótesis pretende ser validada o refutada al final de este trabajo.

De esta hipótesis parten las siguientes preguntas de investigación, con intención de servir de guía para la parte analítica de este trabajo:

1- ¿Existe una relación entre la puesta en práctica de la guerra híbrida y la propia motivación ideológica defendida por parte de Rusia como estrategia antioccidental?

2- ¿Cabe sostener que el discurso ideológico de Rusia, dentro y fuera de sus fronteras, está vinculado a una motivación de demostrar una supuesta debilidad de las democracias occidentales?

3- ¿Se puede enmarcar el caso de Cataluña como muestra de campo de prueba para respaldar tal argumentación?

4- Y, finalmente, ¿Cuáles son los medios usados por Rusia en su injerencia en el conflicto catalán y cómo los podrían perfeccionar en un futuro cercano?

## V. METODOLOGÍA

El método que guía la investigación es el del estudio de caso, teniendo como objetivo fundamental exponer la particularidad de una situación, en este caso la injerencia rusa en el conflicto catalán, para poder determinar una tendencia estratégica mayor, que es la de una guerra no linear por parte de Rusia contra Occidente.

Dada la naturaleza del propio tema y sus objetivos, este caso se puede clasificar como un estudio de caso intrínseco, según Stake (1995), ya que tiene el fin de analizar y comprender un caso en particular, de manera cualitativa. Si se parte de una definición de este estudio de caso según Yin (1993), el presente trabajo se podría caracterizar como una combinación entre un estudio de caso explicativo y descriptivo, al presentar propiedades de ambas categorías.

Para procurar resolver la pregunta inicial de este trabajo, se parte primeramente del concepto principal de "guerra no lineal", más conocido como "guerra híbrida", aunque la concepción de ambos términos se encuentra polarizada e influida principalmente por sus referentes en el ámbito estratégico-militar, cuyas diferencias mayormente descansan en el punto de vista de elección, ergo occidental o ruso. Dichos conceptos, junto con los de la guerra de información y los *fake news*, se van a definir y desarrollar en el apartado dedicado al marco teórico.

Precisar su definición es fundamental, ya que supone el elemento principal de la hipótesis, que trata de exponer la propia existencia de una guerra no lineal, así como concretizar sus supuestos objetivos y fines, particularmente en cara al rol de Cataluña dentro de ésta.
También se ha considerado necesario precisar la posición de Rusia en el mundo actual, dentro del marco de las Relaciones Internacionales (RRII), con sus aspiraciones de potencia regional a una potencia global. Para ello, se indagará en algunos de los aspectos políticos, sociales y culturales más relevantes que han formado el actual estado de la cuestión y dichas aspiraciones. Mediante todo ello, se pretende presentar una mejor comprensión del marco geoestratégico en el que nos encontramos y de los motivos subyacentes que pueden llegar a modelar las estrategias perseguidas por Rusia.

Una vez definidos los conceptos y aclarado el contexto en el cual se encuentra la Rusia actual, se pasa así al estudio de caso. En él se contemplarán tres objetos de análisis separados, los cuales corresponden a diferentes líneas de actuación llevadas a cabo por Rusia en la materia. Juntas forman parte de la estrategia que llevan a una supuesta "desestabilización" – centrado desde una perspectiva político- social – de Occidente, mediante, entre otras cosas, un discurso antioccidental. Estos objetos-medios son: 1. Medios de comunicación estatales; 2. Difusión de información adversa a través de ciberoperaciones u operarios y 3. Difusión de contenidos e influencia política automatizada a través de RRSS. Todos ellos, así se sostiene en este trabajo,

fueron también empleados en la crisis catalana por Rusia - directa o indirectamente. El Estudio de caso además se divide en tres secciones temporales: Pre 1-O; durante 1-O; post 1-O.

En definitiva, la razón de ser del estudio de caso para este trabajo es la de procurar identificar patrones que agreguen valor a la hipótesis de la existencia de una motivación estratégica por parte de Rusia dentro del marco de una guerra no lineal.

## VI. FUENTES

La realización de este trabajo, al tratarse de un estudio de caso, combina varios métodos de recolección de información y se apoya en una amplia base bibliográfica y documental, occidental como rusófila, mayormente proveniente de fondos de la biblioteca de ICADE y de la Universidad de Maastricht, pero también de otras bibliotecas y medios accesibles online.
En términos generales, se puede distinguir entre las siguientes dos categorías de fuentes– las cuales están todas documentadas al final de este TFM, en el apartado "referencias" (véase pág. 60):

En primer lugar, las fuentes primarias. Estas comprenderán, por una parte, documentos de organizaciones internacionales tales como de la UE, Naciones Unidas y por otra parte documentos elaborados por los gobiernos e instituciones gubernamentales en cuestión, tales como el informe del CNI y el documento de Estrategia de Seguridad Nacional rusa. También se incluirán referencias hacia material periodístico, publicado en prensa considerada fiable– basándose mayormente en la cobertura realizada por el diario *El País*, el periódico no deportivo más leído en España en aquel momento y ahora (AIMC, 2021). Es aquí donde es interesante recalcar que el fondo de inversiones *Liberty Acquisition Holdings Corporation* es el principal accionista de PRISA, el grupo editorial al cual también pertenece *El País*. Detrás de este fondo se encuentran personajes relacionados con el partido demócrata estadounidense, por lo que se puede explicar en parte por qué *El País* ha impulsado ofrecer una notable cobertura con respecto a la injerencia rusa en Cataluña. Esto, por ende, constituye también la razón por la cual el presente trabajo va a hacer mayor mención de este diario en concreto que de otros.

En segundo lugar, se hará uso de fuentes secundarias. Estas comprenden libros, monografías, revistas académicas especializadas y revistas de estrategia militar, entre otros.

Es importante destacar que naturalmente existe un amplio sesgo de información en este ámbito, tanto en las fuentes primarias como en las fuentes secundarias, dada la naturaleza controvertida e ideológica del tema y dada la naturaleza de la propia Rusia, puesto que es considerado un país lleno de contradicciones, en el cual, tal como recogía el diplomático estadounidense George Kennan en su momento, no habría que "confundir las 'relaciones exteriores' rusas –que se enmarcan en las instituciones de la comunidad internacional- con su 'política exterior', que pretende devolver a Rusia su estatus de "gran potencia" disputando zonas de influencia {al Occidente}".

# CAPÍTULO II: MARCO TEÓRICO Y ESTADO DE LA CUESTIÓN

## I. MARCO TEÓRICO

### *i. Teoría de referencia en el marco de las RRII*

El marco de referencia teórico escogido está vinculado al del presidente de Rusia, Vladimir Putin, al personificar él el brazo operativo de las políticas externas rusas. Se ha apuntado desde diversos artículos- académicos y no académicos– que a Putin se le podría asignar a la escuela de pensamiento realista, tal como recogen el *Institut français des relations internationales* (Ifri) (Lo, 2018) y otros autores (véase Sumantra (2016) y Bolgov et al. (2019)).

El realismo ha sido la teoría dominante de las RRII a partir de la segunda mitad del siglo pasado. Esta teoría parte de la idea de que los Estados son soberanos y que por ende deberían ser los principales actores en las RRII, y no las instituciones internacionales u otros entes supranacionales (como lo son la UE o la OTAN). En una de las conferencias internacionales más importantes de la historia europea, en el Congreso de Viena de 1814-1815, se defendió el axioma realista de que el equilibrio de intereses fuera el único mecanismo que pueda superar permanentemente las tensiones entre los países. Sin embargo, es aquí donde surge la necesidad de modificar y quizás incluso hasta actualizar la teoría: Basándose en tal hipótesis, consagrada en el Congreso de Viena, se puede observar con facilidad que el del Kremlin *no* es un realismo clásico; el pensamiento del Kremlin se caracteriza por su táctica- es decir, hay un cálculo racional de costes y beneficios para la política nacional. Aquí el Estado se sitúa como estructura que trasmite el ansia de poder a la esfera internacional, rompiendo con la idea original del Congreso de Viena.

Es por ello que el presente estudio de caso se decanta por orientar su análisis acorde con el paradigma teórico del *neorrealismo*, concepto acuñado por Kenneth Waltz en 1979 en su libro “International relations theory”. La principal diferencia entre el realismo y el neorrealismo en las RRII radica en que el neorrealismo centra su análisis en cómo la estructura del sistema internacional determina el comportamiento de los Estados, en lugar de hacer hincapié a los factores humanos e internos, tal y como lo hace el realismo clásico (Joseph, 2014). Según sus criterios correspondientes al enfoque neorrealista, y aplicándolo a Rusia,

apela a una comprensión del sistema internacional con la intención de frenar influencias ajenas a sus intereses en el espacio ex soviético.

### *ii. Terminología y conceptualización*

Antes de indagar y definir los conceptos clave para este trabajo, es necesario destacar que hay que tener cierto cuidado a la hora de emplear conceptos occidentales como los que se van a desarrollar de manera doctrinal y emplear a continuación, ya que pueden dar lugar a una simplificación excesiva y al uso equivocado de éstos como base deductiva para intentar interpretar lo que piensan los estrategas rusos. Sin embargo, es necesario conceptualizar de alguna manera actuaciones recurrentes en el actual escenario geopolítico para aportar cierta claridad analítica y comprender los conflictos contemporáneos- en este caso, aquellos llevados a cabo por entes rusos en territorio Occidental.

Si bien hay un amplio acervo terminológico y conceptual para referirse a la forma aparentemente nueva de conducción de la "guerra" que se suele atribuir a Rusia, la comunidad académica tanto como en el sector militar están lejos de consenso para definir una tipología de conflicto que combina el empleo de medios regulares e irregulares o explicar las aparentemente novedosas tácticas rusas (Colom Piella, 2018).

En primer lugar, no cabe duda de que el término más empleado y popularizado por los medios no especializados en esta materia es el de la "guerra híbrida". Sin embargo, este término ha sido criticado por varios frentes. Según diversos autores y expertos en la materia (véase Murray & Mansoor, 2012), la combinación de diferentes tácticas militares por parte de los actores bélicos difícilmente podría describirse como un fenómeno nuevo que requiriera un término propio como lo hace "guerra híbrida". Históricamente, emplear varios medios en una guerra era más bien la regla que la excepción. Según Schreiber (2016), el término "guerra híbrida" fue empleado por primera vez de manera oficial en la Estrategia Nacional de Defensa estadounidense en 2005, para explicar la combinación de dos o más amenazas de tipo tradicional, irregular, catastrófico o disruptivo (Rumsfeld, 2005). Sin embargo, no fue hasta la publicación del artículo "La guerra del futuro: la llegada del conflicto híbrido" (2005), del general James N. Mattis y el teniente coronel Frank G. Hoffman, cuando término adquirió mayor relevancia.

Años más tarde, el Ejército de Estados Unidos codificó el término en su doctrina de operaciones de 2011 como: "La combinación diversa y dinámica de fuerzas regulares, fuerzas irregulares, elementos criminales o una combinación de estas fuerzas y elementos, todos ellos unificados para lograr efectos mutuamente beneficiosos" (Ejército de los EE. UU., 2011, p.5). Esta amalgama de cuatro elementos definitorios claves de las operaciones vino a establecer lo más cercano a una definición generalmente aceptada del concepto de "guerra híbrida" para las Fuerzas Armadas de los Estados Unidos hasta las acciones de Rusia en 2014.

No obstante, el término tuvo arraigo principalmente con los actores no estatales que luchan contra los Estados y sus métodos, lo que en sí impediría que las recientes injerencias rusas en el extranjero entren en la terminología de la guerra híbrida (Schaufer, 2016).
Más allá, tal como señala el mismo Schnaufer (2016), "la mayoría de las definiciones de guerra híbrida no incluyen los aspectos informativos, económicos, sociales y políticos de la guerra que los Estados pueden aplicar a una escala mucho mayor en comparación con los actores no estatales y con una intención muy diferente".
En particular, al no quedar muy claro hasta qué punto los medios no violentos, como el uso del Internet con fines informativos y desinformativos, forman un elemento constitutivo del término, académicos y expertos, como Galeotti (2015), Kofman y Rojansky, han afirmado que los métodos llevados a cabo por Rusia han entrado en un ámbito que aún no ha sido definido por los estudiosos ni por los funcionarios de defensa (Kofman & Rojansky, 2015).

Es por ello por lo que este trabajo considera preferible el término negativo de "guerra no lineal" (en ruso, *nelinnearnaya voyna*). No obstante, evidentemente, este término tampoco define con suficiente precisión el método que pretendemos examinar, ya que – al igual que el concepto de la guerra híbrida y entre otras carencias – nada en ninguna de las explicaciones da cuenta de una estrategia geopolítica más amplia. Tal como consideran muchos de los expertos en la materia, hacer que el término guerra híbrida o guerra no lineal abarque esta estrategia geopolítica más amplia cambiaría su significado anterior y el concepto. Así pues, si bien las acciones de Rusia dejan cualquier término en entredicho, la elección de éste principalmente se debe al hecho de que, según apunta Mirosevich- Jurasti (2017), supone uno de los tres términos usados por los rusos para referirse al concepto occidentalizado de guerra híbrida. Los otros dos son "guerra ambigua" (*neopredelonnaya voyna*) y "guerra de redes" (*setovaya voyna*).

Dejando de lado las carencias tanto del término guerra híbrida como también el de guerra no lineal para referirse a los métodos llevados a cabo específicamente por Rusia, quedan por aclarar dos otros nuevos términos, frecuente y erróneamente utilizados de manera sinónima: El de *conflicto* híbrido y el de *amenaza* híbrida. Es de relevancia definirlos y diferenciarlos para el objetivo de este trabajo. Para diferenciar estos tres términos y a su vez relacionarlos entre sí, a continuación, se parte de las definiciones dadas en el Documento de Trabajo del Real Instituto Elcano *Amenazas híbridas: nuevas herramientas para viejas aspiraciones* (Galán, 2018). El hecho que Galán haga uso del término de *guerra híbrida* y no de guerra no linear, evidentemente no supone impedimento alguno para usar sus definiciones como base para el subsiguiente desarrollo conceptual. También cabe recordar que el documento de Galán se refiere a estos conceptos de manera general, sin explícitamente relacionarlos con Rusia, por lo que las definiciones son muy genéricas y en sí no directamente aplicables al país. Además, es necesario recalcar que no son claramente diferenciables y por ello deben entenderse como moldes para percibir estructuras en ellas. En definitiva, los tres conceptos quedarían definidos por Galán de la siguiente manera:

Por un lado, la *guerra* híbrida (o guerra no lineal, como preferimos decir a lo largo de este trabajo), acorde con la definición de Galán, es considerada aquí como una "situación en la que un país recurre al uso abierto de la fuerza (armada) contra otro país o contra un actor no estatal, además de usar otros medios (por ejemplo, económicos, políticos o diplomáticos)." (Galán, 2018, p.4). Esta definición coincide la propuesta por Fuerzas Armadas de los Estados Unidos, detallada anteriormente.

Por otro lado, Galán indica que el *conflicto* híbrido supone una "situación en la cual las partes se abstienen del uso abierto de la fuerza (armada) y actúan combinando la intimidación militar (sin llegar a un ataque convencional) y a la explotación de vulnerabilidades económicas, políticas, tecnológicas y diplomáticas." (Galán, 2018, p.4).

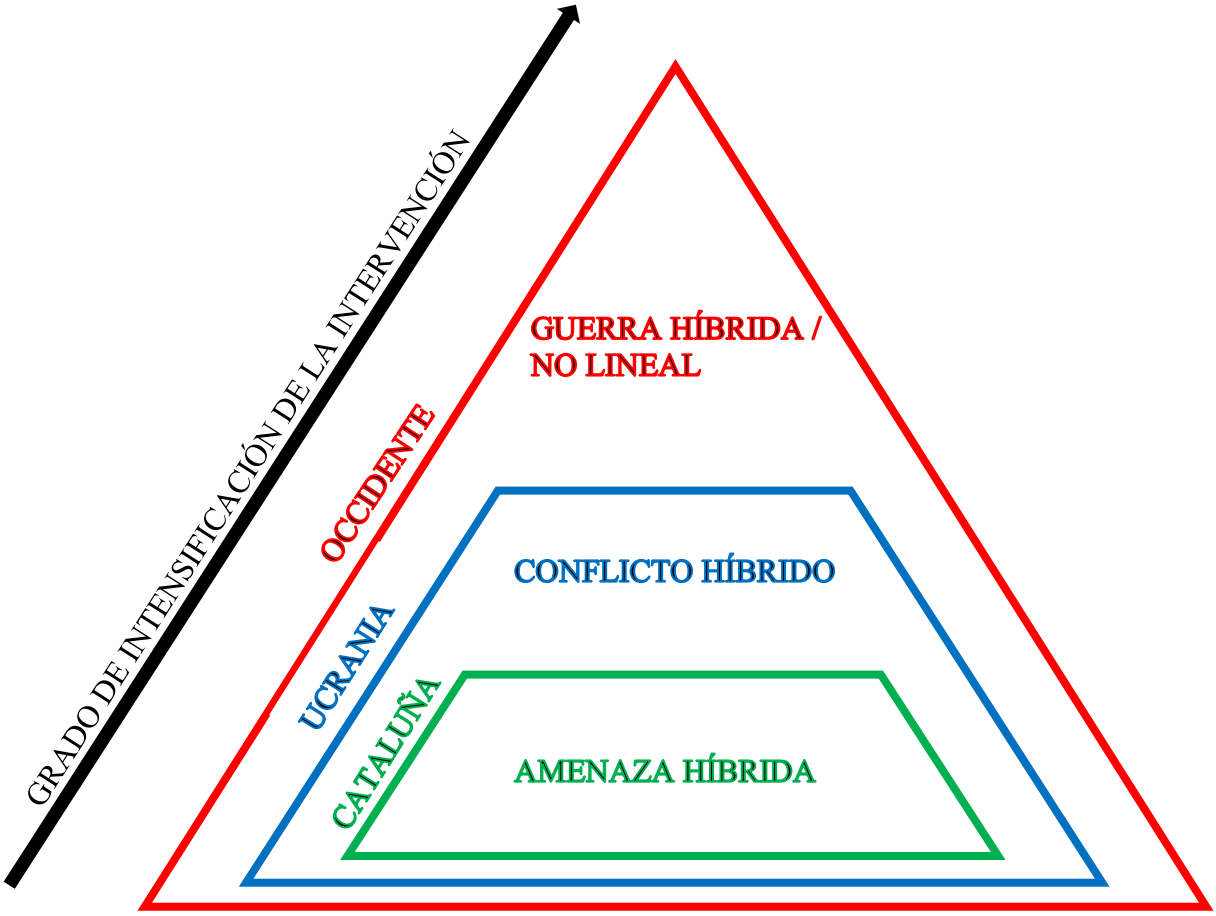
Finalmente, la *amenaza* híbrida es definida como un "fenómeno resultante de la convergencia e interconexión de diferentes elementos que, en conjunto, constituyen una amenaza más compleja y multidimensional." (Galán, 2018, p.4). Es decir, un elemento diferenciador de la amenaza híbrida en comparación con los dos términos anteriores es la ausencia absoluta de medios violentos como instrumento.

Un elemento constituyente de los tres supuestos es el uso de las "medidas activas". Este concepto, al cual Milosevich- Juaristi (2017) llama "militarización de la información" (p. 2), es de larga tradición operativa soviética y combina la "desinformación, propaganda, manipulación y falsificación documental utilizando medios abiertos, semiencubiertos o clandestinos con el objetivo de explotar las brechas sociopolíticas de la víctima e influir sobre ella" (Colom Piella, 2019, p.9). Según el Centro de Estudios Estratégicos e Internacionales (CSIS), el objetivo transcendental de estas medidas activas es "romper la coherencia interna del sistema [político, económico, militar] del enemigo, y no aniquilarle" (Conley et al., 2016, p.10). En la actualidad, el concepto ha sido ampliamente popularizado por la inexistente "doctrina Gerasimov"[3] – llamada así en Occidente – del jefe de Estado Mayor de las Fuerzas Armadas rusas (Galeotti, 2014).

Volviendo a los anteriores tres conceptos esenciales ya definidos para el objeto de este trabajo– guerra híbrida/ guerra no lineal, conflicto híbrido y amenaza híbrida–, es necesario hacer un encuadramiento mejor de éstos para nuestro objeto de trabajo y en particular del estudio de caso de Cataluña y de cómo enmarcarlo dentro de una estrategia de guerra no lineal contra Occidente. Así pues, se ha desarrollado el siguiente modelo gráfico:

[3] En esta misma crónica, Gerasimov sólo describe las estrategias que, según sus observaciones, han perseguido los mismos occidentales: Para los rusos, los que desarrollan las guerras híbridas o no lineales son los occidentales, dando como ejemplo las intervenciones occidentales durante las primaveras árabes y en la guerra de Libia.

**Figura 1:** *Conceptualización de las estrategias de injerencia rusa políticamente motivada en relación con las respectivas áreas geográficas de actuación*




**Fuente:** Elaboración propia

Figura 1 muestra cómo cada uno de los tres conceptos es asignable a un nivel diferente –o mejor dicho, cómo los dos últimos (conflicto híbrido y amenaza híbrida) se pueden encuadrar *dentro* del concepto de la guerra híbrida – como lo llama Galán – o guerra no lineal.

En el primer nivel se encuentra la *amenaza* híbrida. Este primer nivel es identificable con el presente caso de Cataluña, ya que no ha habido utilización alguna de recursos militares por parte de Rusia. Aquí, la estrategia prominente es la que abarca una dimensión informativo-psicológica, en la cual se usan diferentes OI. Esta dimensión es inherente a los tres niveles, pero definitoria en el caso de la amenaza híbrida. Los Estados utilizan las OI en un intento de moldear las percepciones, gestionar las opiniones y controlar el comportamiento (Armistead, 2004). Esto, a su vez, es llevado a cabo mediante propaganda, comunicación estratégica, desinformación o métodos de subversión, para dar forma a un determinado comportamiento

político. El Ministerio de Defensa ruso definió esta "guerra de información" como la capacidad de socavar los sistemas políticos, económicos y sociales; llevar a cabo campañas psicológicas masivas contra la población de un Estado para desestabilizar la sociedad y el gobierno, y obligar a un Estado a tomar decisiones en interés de sus oponentes. Mientras que Occidente considera las OI principalmente como una de las muchas herramientas a la hora de llevar a cabo una campaña militar, para los analistas militares rusos, la información tiene un papel central (Thornton 2015, p. 42).
Más en adelante se analizará en mayor profundidad cuáles son los medios utilizados por parte de Rusia para que constituyan una amenaza híbrida en Cataluña.

En el segundo nivel está el concepto de conflicto híbrido, el cual engloba los medios y las tácticas utilizadas por lo considerado como amenaza híbrida, pero añadiéndole el factor de intimidación militar como también una intromisión "más activa", haciendo por ejemplo uso de la herramienta de presión energética o económica. El conflicto de Ucrania supone un ejemplo real a este fenómeno: Recuérdese la presencia de los llamados *Little Green men* (o "hombres educados", como fueron llamados por la población local coloquialmente) en 2014 en Crimea, inicialmente sin insignia, que resultaron pertenecer al ejército de Rusia con el fin de intimidar a la población "pro-ucraniana".

Finalmente, en el tercer nivel se encuentra el plano más "global", la agudización máxima del enfrentamiento o de la intromisión del actor en forma de una guerra no lineal. Este caso comprende el uso abierto – en lugar de encubierto, por ende, motivando un casus belli – de la fuerza juntamente con otras medidas y amenazas como pueden ser usadas en un conflicto híbrido o en una situación de amenaza híbrida. Para el objeto de interés, se puede atribuir esta última designación de guerra no lineal a las políticas y estrategias perseguidas por Rusia para deslegitimar Occidente. En particular, un ejemplo de confrontaciones abiertamente violentas entre Rusia y Occidente, si nos ceñimos al apoyo de Rusia a Al Asad, es la guerra en Siria. Si bien, a día de hoy, no ha tenido lugar el uso abierto de la fuerza en suelo de ninguno de los dos entes, se puede sostener que se ha hecho uso de *proxies* para llevar a cabo enfrentamientos bélicos, como ya se hizo durante la Guerra Fría– aunque ante un contexto muy diferente, ya que en la actualidad se ausentan los motivos ideológicos de aquel entonces.

En definitiva, el presente modelo pretende a su vez demostrar que el concepto de guerra no lineal es más similar a un proceso que a una guerra propiamente dicha, tal como ya denunciado anteriormente. Entender esto es necesario para poder catalogar el caso de la injerencia rusa en Cataluña como una *parte de* la estrategia "superior", o más amplia, de la guerra no lineal contra Occidente.

## II. ESTADO DE LA CUESTIÓN

### *i. Época soviética*

La actividad rusa en Cataluña no es de ningún modo novedosa en materia, por lo que podemos encontrar diversos casos análogos en la historia moderna y reciente. La lista es extensa e incluye tanto ciberataques como OI, de modo que la siguiente sección no aspira a ofrecer una visión completa y de profundidad.

En particular, vale la pena primeramente hacer referencia a las raíces históricas soviéticas de los actos hoy llevados a cabo por Rusia en materia de injerencias de cualquier tipo en países extranjeros. De este modo, se podrá llegar a comprender mejor la vida política rusa contemporánea y sus métodos de disuasión informativa-psicológica dentro de la estrategia de la guerra no linear.

La historia de la desinformación moderna comienza en el siglo XX con el enfrentamiento entre el comunismo y el capitalismo tras la Revolución Rusa, que llegaría a definir la Guerra Fría (Rid, 2020). Ya entonces, la desinformación – que no la propaganda – se dirigía directamente a la toma de decisiones políticas o se centraba en la manipulación de las percepciones públicas indirectamente. Sin embargo, tal como afirma la gran experta en desinformación soviética, Natalie Grant Wraga, "ningún otro país es capaz como los soviéticos de manipular la opinión pública en Occidente" (Grant, 1990). De hecho, un diccionario de alto secreto del KGB de 1972 define los datos de desinformación como datos especialmente preparados, utilizados para la creación, en la mente del enemigo, de imágenes incorrectas o imaginarias de la realidad, en base a las cuales el enemigo tomaría decisiones beneficiosas para la URSS (Romerstein, 2012).

En plena cúspide de la Guerra Fría, como respuesta a la detección de desinformación soviética por parte de la Central Intelligence Agency (CIA), la administración de Reagan creó

el Grupo de Trabajo de Medidas Activas, un grupo interinstitucional formado por miembros de la CIA, el Federal Bureau of Investigation (FBI) y el Departamento de Estado. El Grupo elaboró importantes informes para el Congreso e informó a la prensa- siendo este el primer intento estadounidense de responder de forma global a la desinformación, de definirla, de crear instituciones para abordarla y de llamar la atención sobre ella al más alto nivel (LSE, 2017). En aquella época, la divulgación de falsa información por parte de la URSS se puede encuadrar como una forma de poder blanco, definiendo "diferentes estrategias de atracción ideológica y promoción de Unión Soviética para cooptar nuevos aliados en la competición entre modelos sociales, políticos y económicos contrapuestos" (Scocozza, 2017, p.64).

Como ha descrito Heller, "dentro de ese conflicto total e incesante que la URSS mantenía contra el mundo capitalista y burgués, la desinformación fue un arma particularmente eficaz, un instrumento capital para condicionar a los individuos" (Volkoff, 1986, p. 170). De hecho, la utilización de la desinformación figuraba un método estratégico de tal importancia para la URSS que, justo antes de la desaparición de esta, el entonces presidente del KGB, Vladimir Kryuchkov, se lamentaba de que los oficiales de inteligencia extranjera, tanto en el Centro (Moscú) como en el extranjero, "subestimaban la importancia y el papel de las medidas destinadas a promover la influencia" y les ordenó mejorar su trabajo en el campo de las medidas activas (Andrew, 2001, p.245).

Vemos que, en la época soviética, los grupos especiales del KGB se preparaban para las exposiciones occidentales. En la actualidad, aunque salvando las distancias, sólo ha cambiado el lugar de las salas de exposiciones al ciberespacio, empleando " (…) narrativas similares, a veces idénticas, para controlar las discusiones en línea (…)" (Gallacher & Heerdink, 2019).

### *ii. Actualidad*

En lo que concierne la historia más reciente, es decir la del siglo XXI, la nueva amenaza apreciada por Rusia – la expansión de los países de la OTAN – ha coincidido con la nueva era de información, cambiando el medio por el cual seguir aplicando sus conocimientos en el ámbito de la desinformación. Sin lugar a duda, hoy en día, Rusia se beneficia de la crisis del periodismo tradicional y los nuevos modelos de negocio o la sobreinformación a través de la

difusión de contenidos sin verificar para mantener el ciclo informativo, maximizar el tráfico u obtener *clickbait* (Martens et al., 2018) con el fin de insertar su propaganda.

Así, se puede identificar el fuerte impacto que han tenido en Rusia las llamadas "revoluciones de colores" – las movilizaciones políticas que se dieron entre 2003 y 2005, en Georgia, Ucrania y Kirguistán, las cuales han demostrado la capacidad de atracción del modelo occidental también en territorios considerados históricamente de pertenencia rusa (Ó Beacháin y Polese, 2012). En estos países ya se efectuaron intromisiones rusas mediante ciberataques y campañas de desinformación (Fontana, 2018), cuya magnitud, debido a la gran interconexión que ha traído internet, no es comparable con las herramientas de desinformación empleadas en antaño. En particular, tras la guerra de Georgia, las fuerzas armadas rusas trataron de implementar el proyecto "tropas informativas", concebido para mejorar las políticas de comunicación militar. Estas "tropas informativas" ya incluían hackers, trolls, periodistas, lingüistas o expertos en marketing y operaciones psicológicas para unificar el mensaje estratégico, complementar las actividades diplomáticas, anticiparse a la cobertura de los medios occidentales, desacreditar las narrativas del adversario, conversar con los internautas o incluso lanzar ciberataques limitados contra los servicios enemigos (Giles, 2016). En el marco de conflictos armados o situaciones de crisis en los que se emplearon de una manera u otra estrategias de desinformación o de disuasión psicológica, también se encuentran en la lista a Estonia, Siria, Chipre y Grecia- aunque en el caso de los últimos dos países mencionados podemos añadir el "arma" complementaria de la presión energética.

No obstante, el probablemente caso más prominente y reciente en este ámbito es la anexión rusa de la península ucraniana de Crimea y el apoyo ruso a los movimientos separatistas en el este de Ucrania. En 2014, Rusia se apoderó– aparentemente sin resistencia– de Crimea y apoyaba a los separatistas en la región ucraniana del Donbás, aunque sin reconocer públicamente este apoyo, dividiendo la población ucraniana en sectores pro-rusos y prooccidentales- o al menos pro-ucranianos. Tal operación ha venido acompañada de un abanico de estrategias, que incluyen desde ataques cibernéticos a la difusión de falsa información. Esta cadena de acontecimientos evidenció un elemento central de la guerra híbrida: La capacidad, para dividir a una sociedad independientemente de la fuerza de sus armas. Ucrania no es el único país afectado de la vecindad rusa: Las campañas de ciberataque y desinformación por parte de Rusia han sido varias y prolongadas en el tiempo.

En lo que concierne a Occidente, en 2016 presenciamos dos de las más importantes y más mediatizadas injerencias rusas en el escenario internacional: Por un lado, la comunidad de inteligencia de EE. UU. Señaló, y ha confirmado en reiteradas ocasiones, que se han llevado a cabo ataques cibernéticos de diversa índole y en elevada cantidad, atribuidos a fuentes cercanas al Kremlin durante y después de la campaña electoral estadounidense. Estas interferencias estarían en parte motivadas para tratar de instalar a Trump como presidente, aunque EE. UU. también ha sufrido ataques a múltiples sectores críticos de infraestructura, como redes de energía, instalaciones nucleares y sistemas de aviación (San Martín, 2019). En la versión desclasificada de un informe publicado conjuntamente por la CIA, el FBI y la National Security Agency (NSA) en enero 2017, se hace referencia al "fuerte consenso" entre las agencias sobre el alcance, la naturaleza y la intención de la interferencia sistemática rusa en nuestras elecciones presidenciales. En el mismo informe, se apunta que evalúa que "Moscú aplicará las lecciones aprendidas de su campaña ordenada por Putin dirigida a las elecciones presidenciales de Estados Unidos a futuros esfuerzos de influencia en todo el mundo, incluso contra los aliados de Estados Unidos y sus procesos electorales." (p.iii). EE. UU. por su parte, impuso sanciones a Rusia en diciembre 2016 – es decir, tras las elecciones presidenciales – por haber interferido en las elecciones[4].

Más recientemente, a finales del año pasado, EE. UU. sufrió un ciberataque sin precedentes a agencias federales, entre ellas, el Departamento de Tesoro y la Administración Nacional de Telecomunicaciones e Información del Departamento de Comercio (Laborde, 2020a). De momento, las investigaciones de los servicios de inteligencia norteamericanos apuntan a que los ataques podrían ser de origen ruso (Laborde, 2021). El portavoz del Kremlin, por su parte, ha acusado a EE. UU. de "rusofobia ciega" (Laborde, 2020b).

Por otro lado, en el mismo año, se pudieron observar noticias falsas producidas por medios de comunicación de origen ruso durante la campaña del Brexit con el fin de influenciar en la opinión pública. Un estudio conjunto de científicos especialistas en datos de la Universidad de California en Berkeley y Universidad de Swansea (Gorodnichenko et al.,

[4] Cabe notar que no se trata de una intromisión completamente sin precedentes: Ya en 1984, el KGB intentó infiltrarse en el partido republicano para obtener información que pudiera comprometer a Ronald Reagan. Tal operación se habría realizado junto con la popularización del eslogan "*Reagan means war*", difundiendo bulos sobre sus supuestas actividades ilícitas y simpatías con macartismo o la crítica a su política exterior, responsabilizándole de la carrera de armamentos y las tensiones con los aliados o su apoyo a regímenes autoritarios (Andrew & Mitrokhin, 2000).

2018), evidencia el uso incrementado de *bots*[5] procedentes de cuentas en Rusia en los días previos al referéndum. Estos *bots* alentaban en gran mayoría a votar a favor del Brexit. Sin embargo, una vez más, Rusia negó implicación alguna, afirmando que tales alegaciones sólo demuestran que Occidente estuviera realizando una campaña contra Rusia.

Las interferencias rusas de esta índole no se ciñen en estos dos países occidentales: así, podemos añadir la demostrada injerencia rusa en el referéndum celebrado en los Países Bajos en 2016 sobre si la UE debería firmar el acuerdo de asociación con Ucrania, en las elecciones francesas e incluso en las alemanas– ambas en 2017– , entre otros casos. El caso de las elecciones alemanas es destacable por su significado: Alemania sigue siendo sin duda una gran potencia, y es considerado en cierto modo el "punto de apoyo del poder en el continente" (Stelzenmüller, 2017, p.3) e inherentemente ligado al proyecto europeo. Su debilitación tendría un valor simbólico importante para Rusia. Es así que Alemania ya ha denunciado explícitamente en varias ocasiones tales injerencias: El jefe del Servicio Federal de Inteligencia (externo) (Bundesnachrichtendienst/BND), Bruno Kahl (BBC, 2016), y el jefe del servicio de inteligencia nacional de la Oficina para la Protección de la Constitución (Bundesamt für Verfassungsschutz/BfV), Hans-Georg Maaßen, han confirmado en repetidas ocasiones que sus agencias están atentas a la intromisión rusa (Reuters, 2017).

Ya en 2015, el informe anual de inteligencia doméstica, publicado por el Ministerio del Interior alemán –el cual supervisa la agencia de inteligencia doméstica Bundesamt für Verfassungsschutz, la Oficina para la Protección de la Constitución – sostiene que "(c)on sus amplios esfuerzos para adquirir información y ejercer influencia, los servicios de inteligencia rusos han actuado durante muchos años con gran intensidad contra los intereses alemanes en Alemania y en la Federación Rusa" y añade que "no hay razón para suponer que sus actividades de espionaje vayan a disminuir en un futuro previsible" (Bundesministerium des Inneren/Ministerio del Interior alemán, Verfassungsschutzbericht, 2015, pág. 256-7). El mismo informe señala en su capítulo sobre las medidas rusas que, además del espionaje de "gran volumen organizativo y financiero", los servicios de inteligencia rusos también "intentan influir en los responsables de la toma de decisiones y en la opinión pública de Alemania" (pág. 254). Asimismo, la propia canciller Angela Merkel ha reconocido públicamente que el gobierno alemán está tomando acción "decisiva" contra los ataques rusos (Deutsche Welle, 2017). Así

[5] Un bot tiene la función principal de amplificar mensajes de forma automática y sistemática mediante el uso de perfiles falsos en RRSS

es que, a pesar de que la campaña electoral alemana no fuera atacada por "noticas falsas" (Shalal & Auchard, 2017), el parlamento alemán aprobó una ley en julio de 2017 que impuso "multas de más de 50 millones de dólares a Facebook y otras compañías de redes sociales que no eliminan contenido ilegal de manera inmediata" (Shuster, 2017).

Dentro de las acciones que engloban la injerencia rusa en las elecciones alemanas, cabe destacar la estrecha colaboración y probable financiación rusa de partidos extremistas en toda Europa, tal como ha sido el caso en Alemania con el partido de Alternative für Deutschland (AfD) (Amann et al., 2019). Una investigación conjunta llevada a cabo por la conocida revista alemana DER SPIEGEL, el canal de televisión pública alemana ZDF, la BBC británica y el diario italiano "La Repubblica" – en gran parte gracias a material proporcionado por el centro de investigación *Dossiercentre* con sede en Londres y financiado por el empresario ruso y crítico del Kremlin Mijaíl Jodorkovski– documenta en profundidad como personajes rusos de alto rango político han desarrollado estrategias para tener a al menos un diputado en el parlamento federal alemán bajo "control absoluto" (Amann et al., 2019). Más allá, se han demostrado diversas visitas y reuniones entre dirigentes de la AfD (véase también Hauteville, 2018) con personas cercanas a Putin, entre ellos Alexandr Dugin, el prestigioso y controvertido intelectual y asesor, al que la revista Foreign Affairs, la revista más importante del *establishment* norteamericano, lo califica – aunque posiblemente de manera exagerada – como 'el celebro de Putin' (Barbashin & Thoburn, 2014).

En el ámbito nacional en España, en lo que respecta la financiación de partidos políticos por el Kremlin, un artículo de *The Economist* apunta a que el partido Podemos podría estar formando uno más en la lista, aunque al tratarse de una "financiación opaca", es difícil de probar (The Economist, 2015). Más allá, aunque España hasta ahora se había librado de mayores ataques cibernéticos directos a sus instituciones, el CNN ha atribuido el reciente ataque al Servicio Público de Empleo Estatal (SEPE), a "un grupo de ciberdelincuentes rusos" (El País, 2021), aunque no se ha podido establecer vínculo con organismos oficiales rusos, a pesar de que inicialmente se hubiese barajado esa posibilidad. Este ciberataque hay que entenderlo como un intento de extorsión geopolítica, ya que las relaciones entre nuestro país y Rusia se han deteriorado significativamente a raíz de las recientes tensiones diplomáticas.

Tal ha sido la actividad irregular rusa en los países occidentales que se han puesto en marcha, por parte de las organizaciones internacionales occidentales más relevantes, ciertos mecanismos con el fin de contrarrestar a lo que se considera ya en cierto grado como amenaza.

Así es que, ya en 2010, la OTAN identificó la amenaza hibrida en el *Multiple Futures Project* – proyecto que pretende hacer un análisis fundamental de los motores del cambio que probablemente afectarán a la Alianza en los próximos 20 años. Con respecto a la amenaza hibrida, su informe recoge que "Psicológicamente, los adversarios utilizarán la conectividad instantánea de unos medios de comunicación cada vez más eficaces para remodelar o rechazar (…) los valores liberales, las ideas y el libre mercado que caracterizan la Alianza. Intentarán obtener una ventaja relativa en el mundo utilizando nuestras normas civiles, los marcos legales y la libertad de los medios de comunicación contra nosotros, mientras manipulan y convencen a otros para que rechacen nuestra forma de vida*"* (p.7).

En cambio, no fue hasta el año 2017 que la UE decide dedicar parte de su presupuesto del Servicio Europeo de Acción Exterior a un *East StratCom Task Force*, un grupo de trabajo creado entre otras cosas con el fin de mejorar la capacidad de la UE para prever, abordar y responder a las actividades de desinformación de los actores externos (EEAS, 2015).
La llamativa tardanza se puede deber a una falta de consenso inicial respecto al trato de la UE con Rusia: Mientras que países como Alemania y Austria priorizan una posición de pragmatismo comercial – fruto de los acuerdos energéticos bilaterales que vinculan a estos países con Rusia –, otros defienden incluir cálculos geoestratégicos en sus relaciones con Rusia (Sánchez Ramírez, 2009).[6] También se creó la unidad *EUvsDisinfo*, la cual, según el *Plan de Acción contra la Desinformación* de la Comisión, "ha catalogado, analizado y sensibilizado más de 4.500 ejemplos de desinformación pro-Kremlin, y ha mejorado significativamente la comprensión de las herramientas, las técnicas y las intenciones de la desinformación por parte de fuentes rusas" (EEAS, 2018).

[6] En el caso de Alemania en particular, cabe mencionar que el antiguo canciller Gerhard Schröder es el presidente del consejo de administración de la petrolera estatal rusa Rosneft, y también mantiene el mismo puesto en el proyecto de gasoducto de gas natural Nordstream 2 - proyecto cuyo único accionista es la también empresa estatal rusa Gazprom (DW, 2020).

## CAPÍTULO III: CONTEXTUALIZACIÓN RUSIA

Las características (geográficas, históricas) propias de Rusia tienen una importante influencia en los factores propios del contexto político y social interno del país y por lo tanto también condicionan la elaboración de estrategias de política exterior. Entender las sensibilidades de Rusia es necesario para llegar a comprender por qué es Rusia el país más involucrado en este tipo de guerras según los datos proporcionados por *Alliance for securing democracy* (ASD, 2021). En esta línea, también es importante remarcar que no se deberían confundir las circunstancias con las causas: Vladimir Putin, si bien el gran impulsor del resurgimiento del Estado ruso por excelencia, no es la causa de la manera rusa de hacer política exterior- la cual es calificada como "agresiva" en muchos artículos. La causa, podemos afirmar, es lo que Lafer (2001) denomina "factores de persistencia": Es decir, aquellos factores – aunque cíclicos en su intensidad– que ayudan a explicar los rasgos importantes de la identidad de un país. Factores, que, en el caso de Rusia, a grandes rasgos, incluirían el profundo sentimiento victimista y revanchista inherente en su sociedad.

Así es que, en los años 90, nos encontramos con una Rusia humillada ante la comunidad internacional: predominaba el descontento y desánimo, de profunda desconfianza en sí mismos, al haber perdido la guerra ideológica, con su consiguiente ausencia de un concepto claro de identidad e interés nacional (Telman Sánchez Ramírez, 2010). Esta sensación sigue en cierta manera vigente en la sociedad y la clase política rusa, ya que, a diferencia de Alemania, en Rusia no ha habido una ruptura radical con el pasado después de 1945: la memoria soviética sigue fuertemente ligada con la identidad del país y su población, como afirma el profesor de Historia en el Instituto Estatal de Relaciones Internacionales de Moscú, Andrei Zoubov (Grynszpan, 2014).

En su transformación de URSS a Federación Rusa, el país sufrió una pérdida territorial y –sobre todo– una gran pérdida de población en torno al 50%. De hecho, ya con el inicio del conflicto entre Armenia y Azerbaijan en 1988, se puso en evidencia el proceso de descomposición del sistema soviético (Vacas Fernández & Calvo Albero, 2005, comp. p. 11). Hay que tener en cuenta que, aunque Rusia es un país muy heterogéneo desde un punto de vista étnico, siempre se ha considerado una gran unidad (la "madre Rusia"). Esta variedad étnica, sin embargo, ha dado lugar a una multitud de conflictos internos a lo largo de la historia: desde

los cosacos en la estepa (que tenían un sentido profundo de vulnerabilidad y aislamiento por lo cual se unían en grupos para sobrevivir y que desarrollaron por ello un sentimiento de hostilidad a los extranjeros) pasando por la amenaza de los súbditos musulmanes en Asia Central, se ha visto continuamente obligada a defenderse. La variedad étnica es considerable hasta en la actualidad: los grupos étnicos minoritarios, de los cuales la mitad son musulmanes, representan casi el 20% del total de la población (Calzini, 2005).

Entre los conflictos contemporáneos que más han marcado a la actual Rusia caben por destacar las guerras chechenas- la primera (1994- 1996) pocos años tras el fin de la URSS- como un punto de inflexión para el devenir de Rusia. Estas guerras fueron fruto de heridas profundas del pasado – de origen histórico, religioso, económico, étnico y de "pura oportunidad" (Vacas Fernández & Calvo Albero, 2005, p.13) – que fomentaron movimientos secesionistas en Georgia, en el Báltico, en Ucrania y también en Chechenia, para culminar, finalmente, en un conflicto sangriento por ambas partes y en lo que iba a ser una crisis humanitaria. Una vez más, un factor interno esencial que concurre para explicar el uso de la fuerza en su momento por parte de Moscú en Chechenia y en otras zonas conflictivas es el "temor de la extensión del conflicto a otras regiones de Rusia" (Vacas Fernández & Calvo Albero, 2005, p.28).

El Kremlin, en su momento, justificó su intervención en Chechenia poniendo el énfasis en la lucha contra la amenaza terrorista[7] y las infiltraciones criminales en el movimiento separatista, en un intento de legitimar sus acciones militares (Calzini, 2005). No obstante, la guerra de Chechenia destrozó la imagen postsoviética de Rusia como democracia pacífica (Higgins, 2019) y la derrota de Rusia exacerbó por otro lado una seria crisis política ya existente tras la desaparición de la URSS. Según Vacas Fernández y Calvo Albero (2005), la atención de esta crisis profunda por la que atravesaba Rusia en los años 90 y sus consiguientes problemas sociales, fue desviada a través de la instrumentalización política del conflicto.

Ante los inicios de una segunda guerra en 1999 y la presión de encontrar un camino propio de salida de esa crisis de identidad (Vacas Fernández & Calvo Albero, 2005), se dio paso al fin de la era Yeltsin – un Yeltsin cansado, enfermo y traumatizado por la primera guerra – y la consecuente entrega al poder a Putin (Higgins, 2019). Putin se alzó al poder prometiendo acabar con los enfrentamientos en Chechenia de una manera victoriosa; Sin embargo, el

[7] De hecho, oficialmente, la guerra fue denominada en Rusia como "operación antiterrorista".

conflicto acabó siendo mucho más largo y complicado de lo esperado para Rusia: la segunda guerra chechena se prolongó durante 10 años y terminó con la declaración unilateral de independencia de Chechenia y la extensión de procesos independentistas más o menos profundos a otras regiones del país (Vacas Fernández & Calvo Albero, 2005).

En la actualidad, Chechenia se encuentra ante una paz muy frágil y engañosa. El que es el presidente de la República de Chechenia desde 2007, Ramzan Kadyrov, y Putin sostienen, de momento, un pacto de carácter de feudo personal. De esta manera, mantienen el delicado equilibrio entre el centro y la periferia, acentuado por las incongruencias de la experiencia federal de las últimas décadas (Calzini, 2005). Además, teniendo en cuenta que Chechenia se ha convertido en un caldo de cultivo para la ideología violenta de Al Quaeda (Higgins, 2019) y que la política exterior de Kadyrov se orienta principalmente hacia el Oriente Medio y el mundo islámico en su conjunto, el líder checheno puede llegar a tener un importante aspecto desestabilizador para Rusia en la era post-Putin.

Más en adelante, la inminente expansión de la OTAN ante sus fronteras fomentó la sensación de cerco estratégico por parte de Occidente. Iniciado con los movimientos sociales de Georgia en 2003, Ucrania en 2004 y Kirguistán en 2005 (Ruiz González, 2013), llevó al país a más situaciones en las cuales consideraba que debía de defenderse ante un enemigo externo. Según el ex Subsecretario de Defensa para Asuntos de Seguridad Internacional estadounidense, Joseph Nye (2014), un país puede obligar a otros a que actúen en beneficio de sus intereses principalmente de tres formas: la coerción, el pago o la atracción. En este sentido, Zubelzú (2007) habla del "externalismo", concepto que "supone una actitud más proactiva y una firme convicción en la necesidad de actuar en pos de la conversión del 'otro'". Sin embargo, a Rusia le queda muy poco del llamado poder blando (equiparable a "atracción", según la terminología de Nye) con el que maniobrar, lo que hace que se comporte de manera agresiva, tal como sucedió en la guerra contra Georgia en 2008 (Karaganov, 2009).

En resumen, el refrán ruso "Rusia nunca comienza las guerras, pero es la que las termina" refleja esta acepción rusa que mezcla un profundo orgullo propio y su percepción de país victimista que actúa de forma defensiva contra Occidente y contra las otras fuerzas que puedan amenazar su soberanía y hegemonía (regional) o su noción de nación-imperio. Además, Rusia sigue temiendo hasta hoy por su integridad territorial y tiene, entre otros, como desafío

interno actual el hecho de que una proporción cada vez mayor de su población musulmana se está radicalizando (Pardo de Santayana, 2017).

Todo esto son algunos de los acontecimientos y fuerzas que nutren el temor histórico del país a ser destruido o aislado y que a su vez fomentan la voluntad del país de volver a la "madre Rusia" y fortalecerse – muy acorde con el pensamiento realista. Como consecuencia, su relativamente humilde PIB (un PIB similar al de Italia) no impide a Rusia gastar de manera desproporcionada en defensa: Según los datos proporcionados por el Instituto Internacional de Investigación para la Paz de Estocolmo (SIPRI, 2021), el gasto militar de Rusia en 2020 supuso un 4,3% del PIB (comparado con el 1,4% en España en el mismo año) – y eso de manera creciente, al tener la sensación de estar viviendo en una situación de emergencia de seguridad nacional. Gran parte de su gasto militar es invertido en intervenciones en Siria, Líbano y Venezuela- zonas que influyen directamente en la seguridad europea y donde Rusia puede actuar como potencial mediador frente a la acción muy limitada de la UE y la falta de resultados de los EE. UU. (Morales, 2015). Todo esto con el fin de demostrar que es un protagonista en la escena internacional, a pesar de los intentos de Occidente de aislar a Rusia mediante la imposición de sanciones (Pascual de la Parte, 2019).

Ante este panorama y la inherente inseguridad y contradicciones internas del país, se entiende – sin ánimo alguno de legitimar – en mayor grado sus reacciones que nos pueden parecer desde Occidente desproporcionadas en el escenario internacional: Se puede sostener que la elección de guerras no lineales reside en la necesidad de adaptación a escenarios que ya no responden a los estándares de las guerras que consideramos convencionales.

## CAPÍTULO IV: ESTUDIO DE CASO

El estudio de caso planteado busca adquirir el conocimiento y las reflexiones más relevantes para la resolución de las preguntas de investigación. Principalmente, su objetivo es proporcionar una mejor comprensión del fenómeno de la amenaza híbrida mediante la descripción de las acciones, principales acontecimientos y su consecuente análisis de las posibles intenciones perseguidas en el ámbito en cuestión por Rusia.

En concreto, este estudio de caso se relaciona con los objetivos definidos para el trabajo de la siguiente manera:

En lo relativo al primer objetivo (motivos de la injerencia de Rusia en Cataluña), se parte de la conceptualización dada en el apartado del marco teórico y se va a presentar una visión temporal de los acontecimientos pre-1-O, durante 1-O y post-1-O, a través de la cual se procurará dirimir las intenciones de Rusia en nuestro objeto de estudio.

En cuanto al segundo objetivo (exposición e interrelación de los conceptos), el estudio de caso profundiza y complementa la comprensión del concepto de amenaza híbrida en concreto – cuya base ha sido principalmente desarrollada en el apartado referente al marco teórico– mediante el estudio más profundo de un ejemplo real, como es la injerencia rusa en el conflicto independentista catalán. Analizándolo, también se tratará de mostrar más detalladamente cómo se encuadra el caso catalán en la estrategia mayor de guerra no lineal como parte estructural de su política exterior, respaldada por la exposición de una supuesta debilidad de las democracias occidentales.

Antes de indagar en las acciones y los acontecimientos específicos que se han efectuado en cada una de las tres etapas establecidas (pre-, durante y post- 1-O) – dentro y fuera del suelo catalán-, es necesario catalogar y exponer, de manera general, estas operaciones – en mayor parte cibernéticas, como parte de las *medias activas*– llevadas a cabo en un sentido de poder blando. En este sentido, Connel y Vogler (2016, p.17) distinguen en un documento de investigación publicado por el centro de análisis naval americano (CNA) entre tres categorías centrales de operaciones cibernéticas (‘ciberoperaciones’), las cuales seguidamente se van a desarrollar en mayor detalle. A su vez, estas categorías van a servir como base para la estructura de cada una de las tres etapas diferenciadas en el conflicto catalán.

## I. Medios de comunicación estatales

La primera categoría, según Connel y Vogler (2016, p.17), corresponde al uso de medios de comunicación pro-rusos financiados por el Estado, como Sputnik, RT (antigua Russia Today) y Russia Beyond the Headlines, entre otros.

La televisión sigue siendo el sector más poderoso de la industria de los medios de comunicación y la principal fuente de noticias para la mayoría de los rusos, aunque su dominio está siendo erosionado por Internet. La cadena de televisión internacional RT, sin embargo, fue creada exprofeso como medio de comunicación destinado al exterior (López-Olano & Fenoll, 2019): RT emite en el extranjero en inglés, árabe, francés y español. Sputnik por su parte, un sitio web de noticias también controlado por el Estado, difunde noticias en unos 30 idiomas (Helmus et al., 2018). El objetivo último de tales medios es, según Margarita Simonián, editora jefe de RT, de la agencia de noticias asociada Rossiya Segodnya y de su servicio multimedia Sputnik, el de "(…) ofrecer un punto de vista alternativo al que dan los medios occidentales" (Yablokov, 2015, p.27). A RT y Sputnik se pueden añadir como principales canales de consumo interno Canal Uno y Rossiya 1 – ambos controlados por el gobierno ruso- como también NTV, cuyo dueño es el gigante energético estatal Gazprom (Beumers, Hutchings & Rulyova, 2009).

En lo que respecta la cadena RT, Elswah y Howard (2020) la consideran como una de las organizaciones más importantes en la economía política global de la desinformación, al ser la organización formal mejor financiada[8] (con presupuesto anual que ronda a los 300 millones de euros (López-Olano & Fenoll, 2019)) y con más personal del mundo que "produce, difunde y comercializa noticias al servicio del Kremlin" (Elswah & Howard, 2020, p.623). El canal se ha establecido en las sombras del sistema mediático soviético y su comportamiento organizativo se caracteriza por los controles de tipo soviético. De hecho, la herramienta online Newsguard, que otorga calificaciones de confianza a los sitios web de noticias en línea, da a

[8] No obstante, el sitio web de RT no revela la propiedad, la financiación ni las estructuras de los holdings (EUvsDisinfo, 2020). Tampoco se proporcionan los nombres de los creadores de contenidos, ni información de contacto o biográfica: RT lo justifica pretendiendo que "sólo los fanfarrones firman sus artículos y pueden ser localizados" (RT France, 2020, 4m16s).

RT una puntuación de 32,5 sobre 100 (25 sobre 100 para la versión francesa), y advierte que el "sitio web viola gravemente las normas periodísticas básicas".

De manera general, se puede afirmar que, desde la crisis ucraniana, los medios de comunicación estatales rusos han intensificado el tono pro-Kremlin y nacionalista de sus emisiones, mostrando de manera más visible su rechazo a la influencia occidental (Roman, Wanta & Buniak, 2017). Estos medios, con narrativas que muestran distintos niveles de sofisticación, son concebidos como una herramienta de poder blando – es decir, operan con la intención de promover internacionalmente la imagen de su país mediante la difusión de propaganda blanca (ergo, gubernamental), tal y como lo pueden hacer muchos otros Estados. También cabe destacar que, hasta fechas recientes, una variedad de periódicos de referencia – como el *Washington Post, New York Times, Daily Telegraph, Le Figaro, Repubblica* o el mismo *El País* (hasta 2016) – incluían periódicamente el suplemento de "Russia Beyond the Headlines" (Colom Piella, 2020). Aquí cabe también notar que los estándares éticos laxos e insuficientes medios a disposición de las plataformas actuales permite al Kremlin (y, por extensión, a sus servicios de inteligencia) emplear numerosos *proxies* para implantar desinformación y falsificaciones en medios neutrales (Darczewska; Żochowski, 2018; Helmus et al., 2018).

No obstante, en el caso catalán, según una investigación de Alejandro Romero, de AltoData Analytics y del profesor Javier Lesaca, RT y Sputnik fueron los mayores difusores de noticias sobre Cataluña (Lesaca, 2017), por lo que el análisis más en adelante se va a concentrar en estos dos medios de comunicación en particular.

Finalmente, acorde con las tres lógicas estratégicas distintas en el ciberespacio, clasificadas por Jensen, Valeriano y Maness (2019), podemos atribuir el objetivo estratégico final del uso de estos medios de comunicación estatales como parte de la "disrupción", concepto que ellos definen como una estrategia diseñada para dar forma al contexto más amplio de la negociación. En este sentido, "el objetivo es poner a prueba la determinación del adversario, señalar el riesgo de escalada y apoyar los esfuerzos propagandísticos de mayor envergadura" (p.5).

## II. Difusión de información adversa a través de ciberoperaciones y operarios

Connel y Vogler (2016) adscriben a la segunda categoría la "difusión de información adversa o engañosa sobre gobiernos e instituciones extranjeras a través de filtraciones de documentos que a menudo se obtienen a través de hackers, *spearphishing*, u otras formas de espionaje" (p.17), aquí adaptado y denominado "ciberoperaciones".

Este tipo de acciones suponen un elemento clave que tiene que ser matizado, ya que – como en casi toda la terminología de esta materia – la concepción rusa sobre el ciberpoder y, por ende, ciberoperaciones, difiere de forma significativa de la perspectiva occidental. Entre estas diferencias, la más destacable es que los académicos y expertos militares rusos conciben la ciberguerra de forma más amplia que los estrategas occidentales. Como es de esperar, también difieren las respectivas perspectivas sobre quién es el agresor y quién es quien se defiende de una campaña cibernética hostil. Sin embargo, en lo que concierne los retos del poder cibernético, los expertos rusos y los académicos occidentales convergen en varios aspectos, como son el dominio de la ofensiva, el secretismo, la difícil trazabilidad, la escalada, etc. (Medvedev, 2015).

Estos mismos aspectos, de hecho, hacen su efecto coercitivo más latente que manifiesto. El espionaje cibernético como estrategia suele ir en paralelo a los esfuerzos de manipulación más amplios, cumpliendo un doble sentido:

En primer lugar, el del acceso a las redes objetivo para el establecimiento de las condiciones para las operaciones de seguimiento. En lenguaje militar, se prepara el entorno para la acción futura. No sólo se accede a las redes críticas y se roba información alterando el equilibrio de la información en una crisis, sino que incluso, si la intrusión se revela, el objetivo se queda preguntando qué más se ha robado y qué otras redes están comprometidas (Jensen et al., 2019).

En segundo lugar, el ciberespionaje ha demostrado ser un medio de bajo coste para manipular la opinión pública. En este sentido, las acciones son una guerra política clásica: el ciberespionaje es "tanto una herramienta para gestionar crisis de forma indirecta como para subvertir la opinión pública y la voluntad política" (Jensen et al., 2019, p.6). Así, en lo que se refiere al referéndum ilegal catalán en concreto, ese año fue "testigo de la explotación que se ha hecho de información obtenida a través de ataques de este tipo con el objeto de influir en la

opinión pública o de las perturbaciones que los agentes de las amenazas —en muchas ocasiones, patrocinados por Estados— han realizado sobre procesos electorales o al socaire de situaciones de conflicto", según el informe del CNN (2018).

Las actividades pueden ir desde la simple penetración en la red para recuperar información hasta la manipulación de datos para corromper la confianza de un rival en sus propios sistemas (Jensen et al., 2019). Estas acciones no son coercitivas en el sentido tradicional: más bien tienen que ver con la competencia a largo plazo y con la forma en que los Estados rivales tratan explotar las asimetrías de información, de manera que se produzcan beneficios de negociación entre ellos. El ejemplo más reciente de presunto espionaje ruso lo encontramos en Alemania, dónde el 18 de junio de 2021 un investigador universitario ruso fue detenido por las autoridades, acusado de pasar información sensible de una universidad alemana a Moscú a cambio de dinero (Generalbundesanwalt [Fiscalía General del Estado alemán], 2021).

Entre los principales actores que operan desde territorio ruso destaca la organización cibercriminal Russian Business Network (RBN), activa sobre todo entre 2007 y 2008 durante el conflicto de Georgia. A esta lista se le pueden añadir CyberBerkut, Energetic Bear, Fancy Bear (o APT28) y CozyBear (o APT29), siendo los dos últimos los responsables del hackeo en las elecciones de EE. UU. en 2016 (Jensen, Valeriano & Maness, 2019). De hecho, la plataforma DCleaks fue creada exprofeso por la inteligencia rusa para apoyar el *hack&leak* del partido demócrata estadounidense (National Intelligence Council [NIC], 2017). En este último caso, sin embargo, el hack&leak se complementó con actividades de inteligencia, propaganda y desinformación en redes sociales – repertorio de actividades que se van a desarrollar en la sección siguiente – e incluso con contactos personales con miembros de la campaña de Trump (NIC, 2017).

Es importante destacar que estos entes criminales suelen operar con el beneplácito del Kremlin y, en muchos casos, directamente como brazo largo de la política exterior: Es así que ha sido confirmado que el RBN mantiene relaciones muy estrechas con el Kremlin (Mshvidobadze, 2017), como ya fue manifestado por el fiscal español José Grinda en 2015.
Aunque algunas organizaciones criminales de este tipo sí que pueden limitarse a adquirir mayormente recompensa económica, las más importantes – con apoyo directo o indirecto del gobierno ruso – tienen como razón de ser la de influir en la opinión pública. Sin embargo, cabe

notar que, como declara el editor ejecutivo de la revista del sector DataBreachToday, Mathew Schwartz, ante el medio independiente Radio Free Europe/Radio Liberty, resulta cada vez más difícil diferenciar, especialmente en lo que respecta a Rusia, entre lo que es ciberdelincuencia y lo que es actividad de un Estado-nación, como el espionaje (Eckel, 2021). El caso de la injerencia en los comicios presidenciales estadounidenses, sin embargo, fue una clara muestra de cómo Rusia aprovecha el ciberespionaje como parte de una campaña más amplia de medidas activas (Hulcoop et al., 2017), alineadas a los intereses del Estado.
No obstante, también es necesario recordar que este tipo de operaciones, aprovechando la línea borrosa entre actividad delictiva cibernética y campaña cibernética patrocinada por el Estado, también es utilizada por la CIA, la Agencia de Seguridad Nacional de Estados Unidos y agencias de inteligencia de todo el mundo.

En el contexto de la divulgación de material obtenido por medios ilícitos y en el contexto del ciberespionaje y las ciberoperaciones en general, hay que incluir el respaldo por operarios concretos, es decir, mediante la mantención de vínculos con agentes que poseen información privilegiada, dispuestos a colaborar con un bando (*whistleblowers*). Ejemplos incluyen a Julian Assange, fundador de WikiLeaks en 2006, y Edward Snowden, el famoso informante que actualmente vive en Moscú y antiguo empleado de la CIA y la NSA – dos individuos, que, aunque no existen vinculaciones concluyentes entre ellos y el Kremlin (así aportándoles probablemente mayor "legitimida"), sí puede afirmarse que, en el caso de la plataforma WikiLeaks, Assange ha sido clave para contribuir a las medidas activas diseminando material obtenido ilegalmente por el Directorado Central de Inteligencia (GRU) ruso para influir en las elecciones estadounidenses de 2016 (U.S. Department of Justice, 2019: 44-49).

Utilizado en conjunción con las otras dos líneas de acción, el espionaje puede ganar acceso para influir en la opinión pública. Estas acciones de conformación no logran concesiones independientes, sino que establecen las condiciones para futuras negociaciones de crisis.

### III. Difusión de contenidos e influencia política automatizada a través de RRSS

La última categoría constituye el uso por parte de Rusia de "trolls" de Internet (es decir, personas a las que se paga para crear blogs y perfiles en línea falsos para inundar las secciones

de comentarios de las noticias y perfiles en línea con puntos de vista engañosos, falsos o pro-rusos a través de diferentes redes sociales). Esta es quizás la parte más visible y también la más denunciada de una posible intromisión rusa: Las redes sociales son un importante factor de polarización y desestabilización de los sistemas democráticos en la era post Trump y Brexit, como lo han señalado Iosifidis y Wheeler (2018).

Rusia tiene órganos semi-institucionalizados para llevar a cabo este tipo de operaciones. Los orígenes de lo que hoy es coloquialmente denominado "ejército de trolls del Kremlin" se remontan a prototipos como la efímera "Escuela del Kremlin de blogueros" de 2009, anterior a la amplia aceptación actual de las redes sociales en Rusia (Giles, 2016).

En la actualidad, la Internet Research Agency (IRA) – agencia popularmente conocida como la "granja de trolls de San Petersburgo" – es un órgano operativo desde 2013, que emplea un millar de trabajadores que participan en medios, blogs, foros o redes sociales. Estos perfiles pueden valerse de medios afines en todo el espectro ideológico que divulgan las narrativas rusas voluntariamente, creando los empleados – profesionales organizados – de 150 a 200 comentarios por persona (cada 12 horas) con los cuales se inundan las redes de contenidos favorables a los intereses del Kremlin (Pintado Rodríguez, 2017).

Se apoyan por redes de *bots* para amplificar el impacto de los mensajes, los cuales pueden emplearse tanto para fines comerciales como para difundir desinformación en múltiples contextos (Colom Piella, 2020). Como ejemplo, en ocasiones, se han lanzado falsas noticias de catástrofes o atentados terroristas a través de Facebook o de *YouTube* que les han permitido medir su propia capacidad para generar el caos entre población y autoridades de los Estados Unidos, principalmente (Chen, 2015). La fiscalía estadounidense califica al IRA como "una organización implicada en operaciones para interferir elecciones y procesos políticos" (U.S. Departament of Justice, 2018) por sus posibles vínculos con la inteligencia rusa – de hecho, la IRA está al mando de Prigozhin, un personaje muy cercano a Putin – y su intromisión en los comicios estadounidenses. Sin embargo, no hay que olvidarse que la IRA también apoya la desinformación y el engaño (*maskirovka*) a nivel militar (Diresta et al., 2018).

Todo esto se lleva a cabo con el objetivo estratégico de alcanzar la "degradación" del otro Estado, lo que es lo mismo que realizar "operaciones coercitivas diseñadas para sabotear

las redes, las operaciones o los sistemas del objetivo enemigo" (Jensen, Valeriano & Maness, 2019, p.5)

Para concluir, es necesario notar que, a pesar de que el autor en el cual esta clasificación se ha orientado, haya concebido la primera categoría ("medios de comunicación estatales") como una subcategoría de ciberoperaciones, en un sentido estricto se puede sostener que esa categoría no es directamente clasificable como tal: más bien, parece más acertado sostener que el conjunto de los métodos relativos a dicha categoría pertenece a una categoría más amplia de OI- catalogable como mera propaganda o herramienta de poder blando del que hacen uso muchos Estados.

## IV. Pre 1-O desde 2012, arranque del proceso de crisis institucional

### *i. Medios de comunicación estatales*

Ya en 2012, en vísperas de las elecciones parlamentarias catalanas, RT publicó una serie de artículos cubriendo el tema de las elecciones y del separatismo catalán. Entre estos artículos se encuentra una breve entrevista con Ferrán Casas y Pere Rusiñol, cada uno defendiendo su posición – Casas siendo independentista y Rusiñol opuesto al proceso secesionista. Si algo destaca de estos primeros artículos de la materia es su relativa imparcialidad. La narrativa realmente se ha ido agudizando en 2016 y 2017, con un visible cambio de tono en favor a la causa independentista mediante un discurso sustentado en parte en noticias falsas o sesgadas: No hay que olvidarse que ambos, RT y Sputnik, son corporaciones que viven de los presupuestos rusos y, para seguir existiendo, deben de demostrar resultados (Zygar, 2016). Un ejemplo de artículo con información sesgada, publicado en este marco temporal, es uno que recoge que Cataluña supuestamente reconocería a Crimea como parte de Rusia (Sabrodin, 2016). En él se cita a Enric Folch, representante del partido Solidaridad Catalana por la Independencia, aunque sin mencionar que este partido no ha estado ni está en el parlamento catalán y, por tanto, no representaba ninguna posición oficial.

### *ii. Ciberoperaciones y Actuación de operativos concretos*

Si bien no hay constancia de ciberoperaciones como los ha podido haber en EE. UU. o durante la campaña del Brexit en Cataluña, sí que ha habido actuación temprana en Cataluña

de operativos concretos de espionaje ruso. En este contexto, caben dos acontecimientos por destacar:

Según un artículo del diario El Mundo, Alexander Ionov, líder del Movimiento Antiglobalizador Ruso se habría reunido personalmente y en varias ocasiones con el político catalán Enric Folch- la primera vez en 2015 en Rusia, con motivo del primer congreso de secesionistas (Colás, 2017). Según el mismo diario, estos congresos con separatistas son organizados por el mismo Ionov, quien recibe financiación del Gobierno ruso, en particular a través del viceprimer ministro ruso Dimitri Rogozin, para promover el secesionismo en Occidente (Colás, 2017). En este primer congreso, parece ser que Folch manifestó su aspiración de celebrar un referéndum para el 2019.

En estos congresos participan representantes de diversos movimientos secesionistas, entre ellos el Sinn Féin, el Frente Polisario o la Liga Norte italiana, el Estado Nacional Soberano de Borinken (Puerto Rico), la Yes California Independence Campaign, el Texas Nationalist Movement, prorrusos de los territorios ucranianos de Lugansk y Donetsk, de Transnistria e incluso el autoproclamado rey de Hawái, Edmund Keli'i Silva Junior. Sin embargo, evidentemente, no está presente ningún movimiento que quiera separarse del Gobierno central ruso ni de ninguno de sus aliados (como podrían ser los tibetanos o kurdos, los tártaros o independentistas del Cáucaso): Las aspiraciones secesionistas en territorio ruso quedan prohibidas por una ley de 2014, por la cual se castiga con cinco años de prisión a todo aquel que promueva tales movimientos.

Por otro lado, Julian Assange, en una llamativa aparición por videoconferencia emitida en la plaza Universidad de Barcelona en septiembre 2017, instó a los asistentes a que la "rebelión en Cataluña se extienda a nivel global" (Segura, 2017), y aconsejó descargarse herramientas para sortear una supuesta censura por parte del Estado de la nación a la sociedad catalana. Además, esbozó paralelas entre la actuación de las fuerzas del Estado para desactivar el 1-O con la represión del régimen del Partido Comunista de China.

### *iii. Difusión de contenidos e influencia política automatizada a través de RRSS*

El uso esta línea de actividad suele concentrarse en el momento álgido de una crisis- inmediatamente anterior o/y inmediatamente posterior a un evento o situación clave de esta, aunque evidentemente también puede estar latente en ausencia de conflicto o crisis visible.

Sin embargo, en el caso del uso de *bots* y *trolls* procedentes de territorio ruso en el conflicto catalán, la actividad más relevante se ha producido en torno al 1-O ("Durante el 1-O"). Esto se refleja en el marco temporal elegido por diversos estudios (como el prominente estudio de Lesaca (2017) que ha recopilado más de 5 millones de mensajes digitales publicados entre el 29 de septiembre y el 5 de octubre para analizar su procedencia y naturaleza).

Al desconocer de la existencia de estudios ni demás publicaciones de tal actividad en el marco temporal que aborda esta sección, difícilmente se puede valorarla con el fin de analizar sus métodos y formas, ni mucho menos exponer su impacto relativo– si tuviese alguno. No obstante, sí podemos asumir razonablemente que ya habría habido cierta actividad de esta índole previa al 1-O, sobre todo teniendo en cuenta que ya antes había habido momentos y situaciones de crispación, como puede haber sido durante las diferentes Diadas (Día Nacional de Cataluña), durante las elecciones autonómicas de 2015, o bien durante la consulta popular no referendaria sobre el futuro político de Cataluña del 2014. Sin embargo, es importante recalcar que no hay pruebas concluyentes y que éstas son meras suposiciones.

## V. Durante 1-O

### *i. Medios de comunicación estatales*

Como es de esperar, la cobertura mediática ha sido particularmente elevada en los meses y días inmediatamente previos al referéndum ilegal del 1-O y durante el mismo. Durante este tiempo, la cobertura por parte de RT ha sido mayor que la de otros medios, según el estudio de López-Olano y Fenoll (2019).

Otro estudio de la presencia de noticias sobre el referéndum catalán en la agenda de las televisiones rusas de emisión nacional, realizado por el grupo de expertos de EU vs Disinfo afirma que "se acusó a Madrid de crear un conflicto artificial y las acciones policiales fueron descritas como brutales y absolutamente inútiles" (EU vs Disinfo, 2017).

Es así que en talkshows televisivos como Rossiya se constataron por ejemplo afirmaciones como que el español se estudia como si fuera un idioma extranjero en Cataluña (Antonov, 2017), o que también las islas Baleares piden la independencia ("El independentismo", 2017). El contenido más significativo entre el sinfín de publicaciones en torno a la señalada fecha ha sido la comparación del referéndum como una "revolución de

color" dentro de la UE y el primer paso hacia su desintegración y, en particular, la comparación del referéndum catalán con el de Crimea; la afirmación de que Occidente era responsable del deseo de los catalanes de independizarse de España por crear las condiciones previas para los movimientos separatistas cuando apoyó y reconoció la independencia de Kosovo; la difusión de imágenes mostrando una supuesta brutalidad policial en Cataluña como respuesta a la celebración del referéndum (que luego resultaron ser parcialmente falsas, tomadas años antes en otras manifestaciones (El País, 2017)); la aserción de que la UE habría ordenado a España llevar a cabo una "acción represiva" para impedir el referéndum, intentando así evitar un debilitamiento de la Unión, y la afirmación de que el uso de la fuerza por parte de la policía haya consistido en violencia deliberada y no en una legítima defensa de la seguridad del Estado, manteniendo que se trataba de una práctica franquista y no de un Estado democrático, entre muchos otros mensajes. Gran parte de estos mensajes han sido recogidos por Milosevich-Juaristi en un artículo para el Real Insituto Elcano en 2017. Llaman la atención las numerosas comparaciones de Cataluña con Ucrania o el Kosovo, en un intento de mostrar el caso de Cataluña como supuesta consecuencia del reconocimiento y el apoyo de la EU a Ucrania y Kosovo.

En otro talkshow televisivo de "Canal Uno" (2017, 9m38s) (Новости на Первом Канале), los presentadores sostuvieron que, como resultado de los enfrentamientos con la policía, unas mil personas resultaron heridas. Estos datos seguramente se basan en los proporcionados por el Departamento de Salud de la Generalitat, publicados en su cuenta de Twitter. Sin embargo, son datos que ya fueron cuestionados en su momento, debido a la forma mediante la cual se habían contabilizado (Parera, 2018). En la misma cadena, se mostró en un telediario del 8 de octubre 2017 el siguiente mapa, donde se puede apreciar una Europa subdividida en varias partes:

**Figura 2:** *Mapa de Europa dividida*


**Fuente:** Canal Uno.

### ii. *Ciberoperaciones y Actuación de operativos concretos*

Del mismo modo que han incrementado las publicaciones relacionadas con la crisis catalana a través de los nombrados medios de comunicación, también se han intensificado la actividad de operativos afines a los intereses del Gobierno ruso en suelo español. En 2019, la Audiencia Nacional inició una investigación sobre la presencia en España de un espía ruso en Cataluña en los días previos al referéndum. Según El Mundo, se trataría de Sergey Fedotov, un oficial de alto rango de los servicios de inteligencia militares rusos relacionado con actuaciones como el intento de asesinato del ex espía ruso Serguéi Skripal en Londres (Marraco, 2019). Tal como han concluido las investigaciones llevadas a cabo por Bellingcat[9], el nombre real de Fedotov es Denis Vyacheslavovich Sergeev de 46 años, licenciado de la Escuela Diplomática Militar de Rusia y miembro relevante del GRU, el Departamento Central de Inteligencia de las Fuerzas Armadas de la Federación Rusa (Rakuszitzky, 2019). En concreto, estaría integrado en el un grupo especial que, según desveló el *New York Times*, funciona bajo el numeronónimo 29155 (Schwirtz, 2019).

Sin embargo, el caso ha sido archivado recientemente, en mayo 2021, por la falta de indicios sobre la existencia de delito (López-Fonseca, 2021).

[9] colectivo internacional independiente que hace uso de la investigación de código abierto y las RRSS para investigar una variedad de temas

Otro personaje relevante en este marco temporal es Julian Assange, el fundador de Wikileaks que también colabora con RT. Al parecer, éste se reunió en diversas ocasiones con varias figuras del independentismo catalán, entre otros con el empresario y editor Oriol Soler, antes e inmediatamente posteriores al referéndum (de Miguel, 2017). Soler, por su parte, considerado uno de los ideólogos y promotores más relevantes del movimiento secesionista en Cataluña, negó en su momento relación alguna entre el encuentro con el ciberactivista y la causa independentista. No obstante, el entonces Ministro de Asuntos Exteriores y Cooperación, Alfonso Dastis, preguntado por este mismo viaje de Soler a Londres, afirmó que hay "muchos indicios" que apuntan a que mediante dicha reunión se habría tratado de manipular información para "afectar" el "desarrollo democrático natural" en Cataluña (Europa Press, 2017).

En lo que concierne Assange, resulta interesante exponer lo que los autores Del-Fresno-García y Manfredi- Sánchez (2018) denominan los "patrones de desinformación" que han encontrado en los tweets del hacktivista. El primer patrón consiste en confundir intencionadamente la parte con el todo. De esta manera, Assange se adhiere a la narrativa y cosmovisión independentista, equiparándola con toda Cataluña ("el pueblo catalán") e intencionalmente ignorando la existencia de la otra mitad de la sociedad, que también es catalana y no independentista, o justificando las decisiones del segmento independentista en nombre de un inexistente, unánime y uniforme "mandato popular". Al mismo tiempo, objetiva al otro bando mediante una simplificación excesiva como Madrid o España. Los autores concluyen que un total de 23 de los 50 contenidos analizados pueden considerarse de este registro.

El segundo patrón responde a la construcción de la percepción de España como una dictadura o como un Estado no democrático: en un total de 27 de los 50 contenidos analizados, Assange cuestiona la existencia de una democracia en España en términos absolutos y lo extrapola a una crisis de la democracia europea- narrativa que se repite en diferentes medios y actores rusófilos, como se verá más en adelante.

El siguiente patrón aspira presentar a Cataluña como lugar donde ocurren acontecimientos extraordinarios: Assange proyecta el movimiento independentista como un subproyecto histórico y a Cataluña como un lugar donde se están redefiniendo las relaciones de poder, preparando el camino para una nueva era. Según el análisis de los autores, once de los 50 contenidos analizados pueden considerarse de este registro.

El cuarto patrón tiene como estrategia exagerar o distorsionar los acontecimientos, pudiendo considerarse 18 de los 50 contenidos analizados basados en hechos parciales. Se modifica la escala real de los hechos para convertirlos en excepcionales o en emotivos partidistas.

A su vez, el quinto patrón presenta información falsa: 16 de los 50 contenidos analizados pueden clasificarse como parcial o totalmente falsos.

Por último, el sexto patrón emplea imágenes como opinión, como herramienta de polarización afectiva: 23 de los 50 contenidos analizados pueden considerarse "performativos" ya que su objetivo es personalizar la política y la polarización afectiva a través de las emociones, y así corroborar la visión del mundo independentista y apagar lo que queda de confianza en los demás utilizando vídeos o imágenes con un fuerte impacto emocional.

### *iii. Difusión de contenidos e influencia política automatizada a través de RRSS*

La utilización de bots provenientes del territorio ruso en el contexto catalán ha sido considerable y denunciado por las autoridades y los medios en varias ocasiones: según el entonces responsable de exteriores, Alfonso Dastis, España había detectado cuentas falsas en redes sociales, la mitad de las cuales podían ser rastreadas en Rusia y otro 30% en Venezuela, creadas para amplificar la causa separatista. Estas acusaciones fueron airadamente negadas por fuentes del Kremlin (López-Olano & Fenoll, 2019). En la misma línea, el think tank del Ministerio de Defensa, el Instituto Español de Estudios Estratégicos (IEEE) sostiene que "el Kremlin está aprovechando el órdago catalán para desestabilizar, empleando para ello una política destinada a generar confusión desde las redes sociales, en una línea similar a la utilizada para influir en las recientes elecciones en EE. UU." (Baqués, 2018, p. 38).

Las cuentas falsas, según un estudio realizado por Javier Lesaca (2017) de la Universidad George Washington entre el 29 de septiembre y el 19 de octubre de 2017 (periodo que comprende las fechas entre el último día de la campaña del referéndum ilegal y la publicación de la carta de Puigdemont a Rajoy en la que amenazaba de someter a votación en el *Parlament* la declaración de independencia de Cataluña), difundían contenidos de RT y Sputnik en las jornadas inmediatamente anteriores y posteriores al referéndum de una manera coordinada. Conjuntamente, habrían distribuido 47.964 publicaciones relacionadas con Cataluña y su contenido se compartió 10 veces más que los publicados por la televisión pública española

RTVE o la Agencia EFE y sus noticias llegaron a tener 1,7 veces más distribución que el diario *El País*.

En general, el estudio refleja que las informaciones de dichos medios se movieron sobre todo entre usuarios partidarios de la independencia. El análisis cualitativo realizado de los 10 enlaces y publicaciones en redes sociales más compartidos de RT relacionados con Cataluña, muestra que RT tenía un interés especial en compartir imágenes y vídeos de personas heridas durante los enfrentamientos con la policía: el 50% de sus 10 posts y enlaces más compartidos denunciaban la actuación de la policía española, un 20% destacó lo mucho que la independencia de Cataluña perjudicaría a la economía española, el otro 20% ofreció un enfoque aparentemente neutral y, finalmente, el 10% criticó y atacó políticamente al presidente del Gobierno español, Mariano Rajoy.

Mientras tanto, los 10 posts más compartidos del grupo Sputnik sobre Cataluña favorecían la narrativa de los grupos independentistas catalanes. De ellos, el 40% denunció la actuación de la policía española, un 30% criticó al presidente del Gobierno español y el 30 % señaló el apoyo internacional a la independencia de Cataluña.

Por otro lado, en lo que concierne los perfiles que comparten dicho contenido, Lesaca muestra que sólo nueve de las 100 cuentas más activas parecen seguir un comportamiento humano en sus estrategias de publicación e interacción. Otras siete cuentas corresponden a perfiles oficiales en las redes sociales de RT y Sputnik y las 84 cuentas restantes no pueden identificarse con ninguna persona o institución real, ya que no generan ningún contenido o publicación original y propagan enlaces y publicaciones en redes sociales de otros de forma constante, sistemática y masiva, utilizando en la mayoría de los casos a RT y Sputnik como fuente principal.

Lesaca procede diciendo que todo ello indicaría con rotundidad que en el 84% de las cuentas clave que difundieron de forma sistemática y masiva los contenidos de RT y Sputnik sobre Cataluña se trataría con gran probabilidad de bots digitales- algunos de ellos publicando el mismo contenido al mismo tiempo, y otros publicando una media de 1425 mensajes al día, lo que refuerza la hipótesis de que se trata de bots digitales que ejecutan una estrategia coordinada.

Lesaca divide esta red de perfiles digitales anónimos en tres grupos: el primer grupo, que aborda el 24% de estas cuentas, parece mostrar claramente simpatía hacia el régimen de Nicolás Maduro y Hugo Chávez en Venezuela. El segundo grupo, con el 37,7% de las cuentas, se dedica casi exclusivamente a redistribuir o "retuitear" contenidos de RT y Sputnik. Sin embargo, a diferencia de las cuentas relacionadas con el movimiento "chavista", este segundo grupo se esconde bajo identidades encubiertas bien elaboradas. El último grupo, el 27,3%, distribuye y "retuitea" masivamente contenidos publicados por varios medios de comunicación internacionales, no sólo RT y Sputnik. Twitter ha ido eliminando una parte de las cuentas más activas. El informe concluye que "los conglomerados mediáticos rusos *RT* y *Sputnik* han participado en una estrategia deliberada de disrupción en la conversación digital global sobre Cataluña".

Cabe notar que el de Lesaca, si bien quizás el más citado, no es el único estudio que se ha realizado en lo que concierne la naturaleza de la difusión de mensajes relativos a Cataluña de RT o Sputnik: La empresa de analítica de RRSS, *Audiense*, confirma el mensaje de los resultados aportados por Lesaca, aunque reduce el número de bots existentes a la hora de difusión de mensajes sobre Cataluña de la cadena RT o la agencia Sputnik a 13 sobre 100, un 13%, lo que equivaldría a 4883 cuentas "no operadas manualmente" (Galán, Abad Liñán & Alameda, 2017). No obstante, el estudio de Lesaca parece ser el más completo, por lo que se ha decidido mencionar el de *Audiense* al margen, con el único fin de contrastar en cierta medida los datos aportados.

## VI. Post 1-O

### *i. Medios de comunicación estatales*

Tras el fallido intento de referéndum del 1-O, los medios rusos no han cesado sus publicaciones al respecto, aunque sí orientándolo más a un discurso de negación sobre su presunta influencia en la opinión pública durante la celebración de algunas elecciones y referéndums. Tal copiosa contranarrativa, en especial de RT, se podría deber a la amplia cobertura mediática de diversos medios, como *El País*, a las acusaciones de manipulación por parte de los medios de comunicación rusos de la opinión pública, por lo que desde RT "no tardaron en contraatacar denunciando el acoso y adoptando una postura victimista" (López-Olano & Fenoll, 2019, p. 4).

Las publicaciones más destacables incluyen un video de RT Francia (2019) en el cual se aseguraba que el presidente francés Emmanuel Macron difunde noticias falsas (*fake news*) sobre sobre la injerencia rusa en los referendos del Brexit y de Cataluña. Anteriormente, Macron, durante un debate, había manifestado su preocupación sobre lo que el consideraba una manipulación de los votos en estos referéndums por potencias extranjeras. En RT France, estás manifestaciones se han calificado como "carecientes de pruebas" (1m45s), a pesar de que, en aquel momento, numerosas autoridades ya habían confirmado y denunciado tal injerencia procedente de territorio ruso – si bien de diferentes intensidades y formas. Como ejemplo, unos meses antes de las afirmaciones realizadas por Macron, el Parlamento británico publicó un informe especial en el que se presentaron pruebas de la intromisión rusa en los referendos del Reino Unido y de Cataluña[10].

Unos meses más tarde, Sputnik (2019) publicó un artículo alegando el rechazo por parte del Alto Representante de la UE para Asuntos Exteriores, Josep Borell, a la lucha contra el separatismo en la UE. Si bien no se trata de una noticia falsa en un sentido estricto, Sputnik claramente ha distorsionado las declaraciones de Josep Borrell realizadas durante una entrevista con Radio Nacional Española (RNE). En esta entrevista, Borrell se refería exclusivamente al separatismo en Cataluña, mientras que, en el artículo de Sputnik, se presenta ambiguamente como una declaración sobre el movimiento separatista dentro de la UE en general. Borrell únicamente dijo que enfrentarse al movimiento independentista catalán no formaba parte de su nuevo trabajo, porque "es un problema interno de un país miembro" y "no es un papel para el Alto Representante de la Unión Europea en Asuntos Exteriores" (DW, 2019).

Otros artículos que llaman la atención están relacionados con la reciente detención del líder de la oposición rusa Alexei Navalny, comparándola con la orden de detención a los líderes independentistas catalanes (Rodríguez García, 2021). Los artículos, ambos publicados en febrero de 2021 por Sputnik y RT respectivamente, consideran que las sentencias de prisión tienen motivos políticos y sostienen que los tribunales de Alemania y Bélgica pidieron a las autoridades españolas que anularan tales sentencias. Además, afirma incluso que la legitimidad del Tribunal Supremo español fuese cuestionada por "toda la UE" (Rodríguez García, 2021).

[10] El informe del Parlamento hace referencia a la investigación realizada por la agencia "89up"

No cabe duda de que esta serie de afirmaciones son un intento de desviar cualquier crítica sobre la detención y el encarcelamiento de Navalny en este caso y la represión de los manifestantes que protestaron por ello. Evidentemente, ninguna de las dos principales afirmaciones de este artículo es cierta: si bien los tribunales de Alemania y Bélgica rechazaron la extradición a España del líder independentista catalán y expresidente regional Carles Puigdemont en 2018, lo hicieron por razones técnicas. En ningún momento ninguno de esos tribunales ha pedido a las autoridades españolas que "anulen las sentencias por motivos políticos" ("La UE niega comparaciones…", 2021) contra los dirigentes catalanes, al contrario de lo que llegó a afirmar el ministro de Exteriores ruso, Serguéi Lavrov, en su rueda de prensa.

Más allá, RT distribuyó un llamativo informe realizado por M.C. McGrath (2018), fundador de una organización radicada en EE. UU. denominada Transparency Toolkit, que pone en duda la metodología de Lesaca y otros. Se trata de un informe remitido además al Parlamento Británico y accesible por tanto a través de su web. Afirma que: "la desinformación no es una técnica exclusiva de Rusia, Venezuela o cualquier otro país .... Es necesario explorar cómo las propias afirmaciones de noticias falsas pueden usarse como una táctica manipuladora y comprender el impacto que esto tiene en la sociedad" (McGrath, 2018).

El mismo medio publicó un artículo a finales de 2017 afirmando que la inteligencia española no había "detectado ciberataque ninguno, por parte de ningún Estado, durante el conflicto en Cataluña" (RT, 2017). Sin embargo, en aquel momento, las investigaciones judiciales al respecto estaban lejos de concluir.

***ii. Ciberoperaciones y Actuación de operativos concretos***

De momento, no se ha demostrado la existencia de filtraciones (sean de la naturaleza que sean) o sabotajes significantes por parte de Rusia – o, por lo menos, no hay documentos desclasificados que indiquen tal cosa – en lo que concierne nuestro objeto y el marco temporal post 1-O en particular.

Sin embargo, sí que se sabe, a raíz de una investigación judicial de octubre 2020 relativas al desvío de subvenciones para la causa separatista, que un "grupo ruso" se ofreció el 24 de octubre de 2017 a enviar 10.000 soldados a Cataluña y pagar toda la deuda catalana para ayudar a la región a lograr la independencia en 2017 (García, 2020). Según las investigaciones, Víctor Terradellas, hombre de confianza de Puigdemont y su enlace en asuntos internacionales,

desveló este dato en unas conversaciones telefónicas mantenidas con Xavier Vendrell, ex miembro del gobierno catalán y ex miembro del grupo terrorista disuelto *Terra Lliure*, añadiendo que Puigdemont rechazó la oferta. Terradellas mantuvo varias conversaciones con el delegado de dicho "grupo ruso" y demás personalidades rusas: En mayo de 2018, debía viajar a Rusia para una reunión, presuntamente con ese grupo, a fin de desarrollar una plataforma de criptomonedas con el objetivo de "garantizar la estabilidad financiera" de la Generalitat y "evitar el control del Estado en los movimientos de capital", según el auto judicial (García, 2020). Sin embargo, fue detenido pocos días antes, por lo que no pudo asistir. El mismo juez que lleva la investigación señala que "las reuniones y contactos del grupo sirvieron a la estrategia de desinformación y desestabilización" contra la UE (García, 2020).

Desde luego, la oferta respecto al envío de 10.000 soldados rusos a la región autónoma resulta preocupante, ya que, de haberse aceptado, la injerencia rusa hubiese tomado una dimensión diferente, dando el paso de una amenaza híbrida, a la de un conflicto híbrido (o peor), como es el caso en Ucrania.

***iii. Difusión de contenidos e influencia política automatizada a través de RRSS***

En 2019, cobró importancia en Cataluña un movimiento llamado *Tsunami democrátic*. Esta plataforma se dedica a organizar y coordinar protestas y acciones callejeras a través de sus cuentas de *Twitter*, *Instagram* y su canal de *Telegram* como respuesta a la publicación de la sentencia del procés. Tiene una organización sofisticada y, en palabras del director de estudio de comunicación *LaBase*, Àlex Comes, es "la última evolución del activismo político" (Terrasa, 2019), ya que, a contrario de una campaña política convencional, son los propios activistas los que general y comparten contenido político.

Si bien poco o nada sabe el público, de momento, sobre su fundador y quién está detrás, no hay que descartar que, en la divulgación de sus mensajes vía las distintas mensajerías instantáneas, estuviera la plataforma apoyada en parte por *bots*, aunque no hay nada probado de momento.

Sin embargo, en lo que concierne a Rusia, en noviembre de 2019 se conoció que meses antes se habían iniciado investigaciones sobre posibles vínculos entre *Tsunami Democrátic* y la inteligencia rusa (Efe, 2019), aunque, al tratarse de investigaciones bajo secreto, no ha

transcendido apenas informaciones al respecto, además de que el caso ha sido archivado recientemente, en mayo 2021.

Al tratarse de una plataforma que fundamentalmente opera por mensajería instantánea y RRSS, se ha optado por incluir esta presunta involucración rusa en las secuelas del conflicto catalán en este apartado, aunque también se podría haber situado perfectamente en el apartado anterior (II).

Como modo de resumen de todo lo precedente, el siguiente modelo gráfico de la Figura 2 pretende condensar los aspectos inherentes a las líneas de actuación anteriores, diseminadas en cinco tipos de medios o herramientas detectadas a lo largo del estudio de caso.

El modelo está basado en el desarrollado por Galán (2018) en su documento de trabajo publicado por el Real Instituto Elcano, aunque se han tomado ciertas modificaciones para aplicarlo al caso presente de Cataluña.

Las cinco herramientas – apoyadas en el Informe Especial del Global Engagement Center (GEC, 2020) – que se han optado por destacar en la siguiente Figura 2 son:

Primero, las "comunicaciones oficiales del Gobierno": éstas incluyen declaraciones del Kremlin o Ministerio, publicaciones oficiales en las RRSS rusas, y declaraciones de funcionarios rusos. Aquí se podrían consignar las declaraciones de varios representantes rusos (desde Lavrov, el ministro de Asuntos Exteriores, a Korchagin, el embajador ruso en España, pasando por el mismo Putin), considerando el conflicto catalán como un "asunto interno" e incluso expresaron oficialmente su "total apoyo a la integridad territorial de España" y afirmaron que Rusia carecía de interés absoluto en participar en el conflicto (Milosevich-Juaristi, 2017).

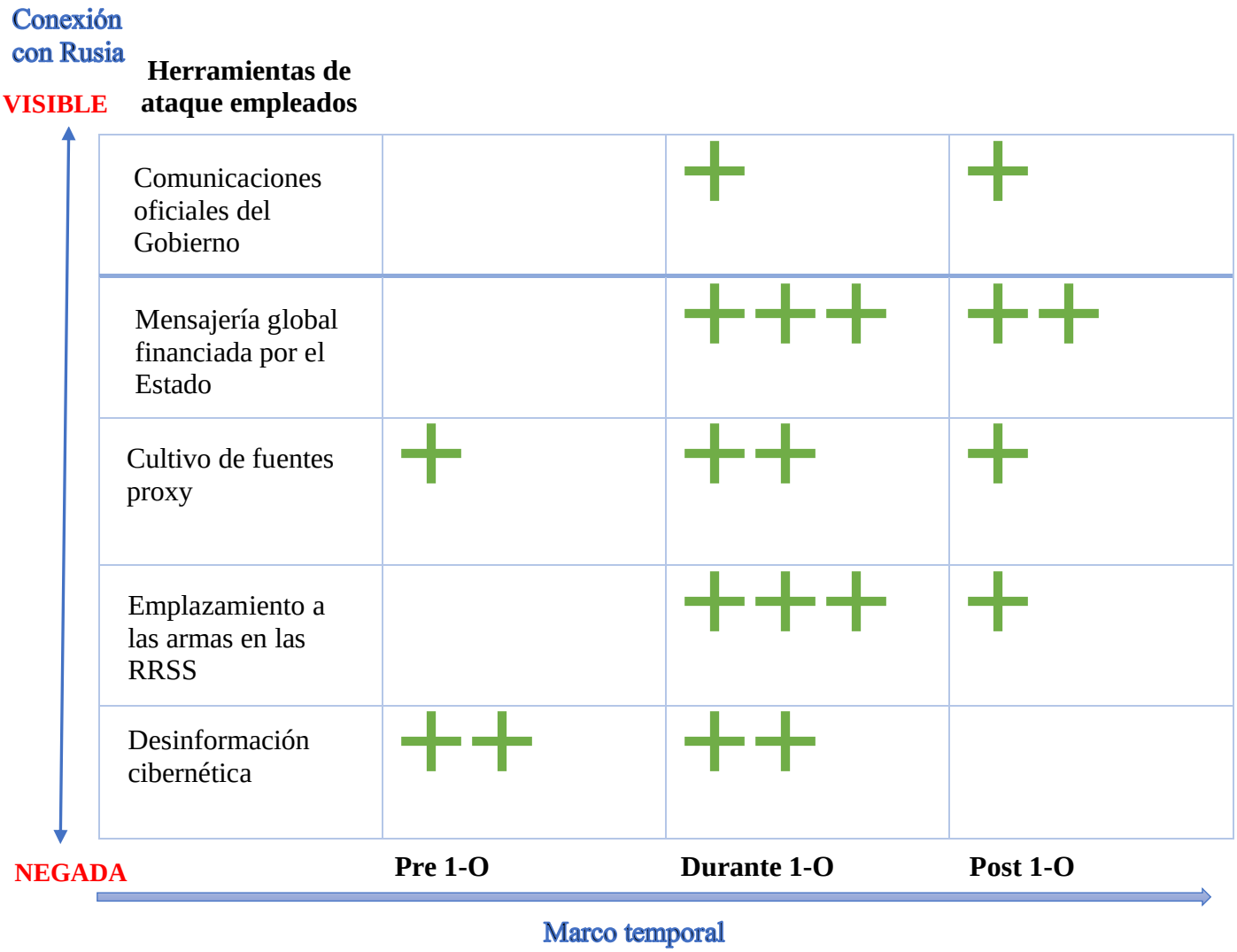
Segundo, bajo "mensajería global financiada por el Estado (ruso)" se entienden los medios de comunicación financiados por el Estado y orientados al extranjero y sus derivados, o también instituciones socioculturales internacionales rusas.

Tercero, la herramienta de "cultivo de fuentes proxy" abarca los medios alienados con Rusia con alcance global, proliferadores – voluntarios como involuntarios– de la manipulación de las narrativas rusas y la amplificación de la narrativa del Estado extranjero.

Cuarto, el "emplazamiento a las armas en las RRSS" se traduce en campañas permanentes para socavar la fe en las instituciones y la amplificación de protestas o discordia civil.

Finalmente, la "desinformación cibernética" incluye el hackeo y la consiguiente publicación de información sensible, la clonación de un sitio web, falsificaciones, interrupción de fuentes oficiales o medios objetivos.

**Figura 3:** *Modelo de amenazas híbridas: Aplicación al caso de Cataluña*




**Fuente**: Elaboración propia.

A falta de espacio para asignar a cada una de estas cinco herramientas los correspondientes ejemplos presentados a lo largo del estudio de caso, se ha optado por ceñirse a mostrar la intensidad del uso de las respectivas herramientas mediante el icono verde (uno para menor intensidad hasta tres para mayor intensidad). Las casillas vacías son aquellas en las cuales no se ha encontrado suficiente información pública al respecto, por lo que no se puede proceder a evaluar su intensidad.

Cabe notar que todo lo representado en Figura 3 son aproximaciones y tiene el mero fin de simplificar y facilitar una visión general de los hallazgos presentados. A modo de sugerencia para futuros estudios, se podría ampliar el modelo para precisar las vulnerabilidades atacadas e identificar los déficits e insuficiencias inherentes a nuestro sistema.

# CAPÍTULO V: CONCLUSIONES

Para validar o refutar la hipótesis principal planteada al inicio del trabajo, se procederá primero a retomar y comentar las preguntas de investigación acorde con los aspectos que han ido surgiendo a lo largo del análisis realizado.

Las preguntas de investigación se pueden dividir en dos categorías temáticas: dos (pregunta 3 y 4), se ciñen al objeto de Cataluña en particular (y con ello a la amenaza híbrida) mientras que las otras dos (pregunta 1 y 2), se encuentran en un plano más elevado, el de una supuesta guerra no lineal contra Occidente. Por ello, esta sección está dividida acorde con estas dos líneas de investigación- las cuales, sin embargo, no hay que verlas como cuestiones separadas sino, al contrario, se refuerzan mutuamente.

## I. Injerencia en Cataluña como amenaza híbrida

La primera pregunta de investigación planteaba si resulta posible enmarcar la injerencia rusa en el caso de Cataluña como muestra de campo de prueba para demostrar una supuesta debilidad de las democracias occidentales.

En base a las conclusiones de los análisis realizados, es posible afirmar que la crisis catalana ha sido, desde luego, instrumentalizada por los medios estatales rusos para respaldar cierto discurso antioccidental e incluso antidemocrático y, expoliando el conflicto al plano europeo, exponer una supuesta fragilidad e incoherencia de la UE. Más allá, a través del estudio de caso hemos podido corroborar como el caso catalán encaja en el concepto de "amenaza hibrida" (véase Figura 1) y como es, aunque no el único campo de batalla, pero sí una pieza dentro de la desacreditación a Occidente.

Ligada a esta pregunta, se encuentra la pregunta 4 de investigación que buscaba conocer los medios usados por Rusia en su injerencia en el conflicto catalán y cómo los podrían perfeccionar en un futuro cercano.

En el estudio de caso se ha procurado exponer las estrategias o, mejor dicho, las líneas de actuación más relevantes y empleadas en un contexto de amenaza híbrida, como es el caso catalán. En particular, Figura 3 presenta un resumen de tales medios utilizados antes, durante y después del punto álgido de la crisis catalana.

## II. Injerencia en Occidente como guerra no lineal

Del mismo modo se puede responder la siguiente pregunta de investigación, que cuestiona si existe una relación entre la puesta en práctica de la guerra no lineal y la propia motivación ideológica defendida por parte de Rusia como estrategia antioccidental, de manera afirmativa.

Esta afirmación se sustenta en dos pilares: por un lado, en la sección referente al estado de la cuestión se ha podido vislumbrar cómo este tipo de aspiraciones, incorporadas bajo el término de "guerra no lineal", históricamente, solían llevarse a cabo en un contexto de confrontación entre Rusia y lo que representa Occidente. Por el otro lado, aunque se ha mostrado que no existe una definición inequívoca del término de guerra no lineal, lo establecido en el apartado de conceptos del marco teórico apunta a la existencia de cierta motivación ideológica, de naturaleza antioccidental, a la hora de llevar a cabo actuaciones de esta índole, al menos cuando hablamos de Rusia.

Finalmente, la pregunta respecto a si cabe sostener que el discurso ideológico de Rusia, dentro y fuera de sus fronteras, está vinculado a una motivación de demostrar una supuesta debilidad de las democracias occidentales, también se puede responder de manera positiva. A lo largo del trabajo, se ha manifestado que, desde el punto de vista estratégico, el beneficio para Rusia ha consistido en provocar el caos en su objetivo. Esta táctica clásica de las OI, como hemos visto en el estudio de caso, se ha llevado a cabo mediante métodos de degradación, disrupción y desacreditación (Jensen et al., 2019) – estrategias (o probablemente mejor dicho, tácticas) de manipulación que se han desarrollado en varios frentes, con el fin de obtener efectos en situaciones en las que Rusia tiene pocas ventajas.

El objetivo final de esta pretensión de querer demostrar una supuesta debilidad de las democracias occidentales tiene una doble dimensión:

Por un lado, evidentemente tiene el esperado fin de que estos esfuerzos sirvan para que Occidente llegue a considerar a Rusia a la par y pueda sentarse en la mesa de negociación. Las relaciones entre Rusia y Occidente han sido debatidas en numerosas ocasiones y no parecen tener una solución a corto ni a medio plazo, por lo que tampoco es de esperar que este tipo de ataques cesen.

Por otro lado, les vale de consumo interno con el fin de legitimar de alguna manera la fuerte tendencia autocrática que tiene el liderazgo de Putin. Así, por ejemplo, la actual pandemia mundial que estamos viviendo le serviría a Putin como buen medio propagandístico: El director de investigación en la Henry Jackson Society de Londres, Andrew Foxall, afirma que "Putin lleva mucho tiempo argumentando que la democracia no es el paraíso que Occidente proclama, y en las crisis actuales las democracias del mundo no parecen ser más efectivas que las autocracias en hacer frente a la expansión del coronavirus" (Dixon, 2020) – al fin y al cabo, como dice Milosevich-Juaristi (2017), el "antioccidentalismo" es uno de los pilares que sustenta el régimen ruso.

Al hilo de todo esto, la hipótesis planteada - la existencia de una estrategia antioccidental perseguida por Rusia, reflejada en la denominada "guerra no lineal", con el fin de desestabilizar Europa, a través de una injerencia en el conflicto independentista catalán- puede ser aceptada en términos generales.

Sin embargo, se requieren ciertos matices y comentarios para poder ser validada, aunque siempre con cierta cautela, en su plenitud: primero, visto las maneras en la cuales Rusia perpetúa sus acciones, no parece acertado catalogar éstas como "una estrategia", entendida como unificada y coherente. Al contrario: son varios los autores que alegan que el comportamiento ruso en el plano de las RRII (en el sentido más amplio de la palabra) tiene como cualidad fundamental el oportunismo táctico (González Levaggi, 2020).

Segundo, hay que hacer constar que las OI no son propiedad del Kremlin, sino que también son consustancial en la cultura estratégica occidental y (quizá de una manera particularmente agresiva) china y que "cualquier actor —aliado, neutral o adversario— también puede hacer «cosas» híbridas para proyectar su influencia y mejorar su posición relativa en el mundo actual" (Colom Piella, 2019, p.14).

Tercero, la terminología de "desestabilizar" Europa, a pesar de ser un término empleado ampliamente en el mundo académico y no académico, puede resultar ambigua, por lo que habría que encontrar una manera para medir el impacto de este tipo de medidas para definir el término correctamente.

Cuarto, y, para terminar, aunque ya haya sido señalado anteriormente y pueda resultar evidente, Cataluña no es ni el único, ni probablemente el más relevante objeto de injerencia

rusa en suelo europeo. Tampoco hay que olvidarse de que el hecho que las medidas activas puedan desparecer puntualmente del foco mediático, no quiere decir que hayan cesado. Por ello, quizás no sea demasiada osadía presumir que, en una intensidad u otra, las medidas activas siguen *activas*- tanto en Cataluña como en otras regiones y planos.

**III. Perspectiva y recomendaciones**

De cara al futuro es de esperar que, con el progresivo desarrollo de la tecnología, se presentarán nuevas oportunidades a las amenazas híbridas (y por ende, a los conflictos híbridos y las guerra no lineales) y que nuevos agentes tratarán de aprovechar el creciente poder de manipulación del ciberespacio (Galán, 2018). Una tendencia alarmante, aunque muy incipiente, es la de los llamados *deepfakes*. Parafraseando a Nina Schick (2021), periodista de investigación en temas de *deepfakes* y autora de un libro con el mismo título, los *deepfakes* son un tipo de medios de comunicación sintéticos. Estos son esencialmente cualquier tipo de medio de comunicación (puede ser una imagen, un vídeo o un texto) que se genera por inteligencia artificial (IA). De momento, sin embargo, sólo nos encontramos al principio de la revolución de los medios sintéticos: sólo en los últimos cuatro a cinco años ha sido posible crear este tipo de "medios fake" y en los últimos dos años hemos visto cómo su aplicación en el mundo real se ha filtrado desde fuera de la comunidad de investigación de la IA. La experta alega que, en el futuro, todos los medios de comunicación van a ser sintéticos, ya que cualquiera podrá crear contenido con un grado de fidelidad que ahora mismo sólo es posible para los estudios de cine, y podrán hacerlo sin apenas coste.

Estas evoluciones conllevan una incluso mayor dificultad de trazabilidad, por lo que será necesario potenciar los esfuerzos para defenderse de los ataques a una sociedad abierta. Estos esfuerzos, como bien dice Galán (2018), deben de llevarse a cabo en varios ámbitos y planos simultáneamente. Entre los cinco que señala (p.23), hay dos que caben destacar a continuación:

En el plano jurídico, no sólo se debería definir su encaje legal en el ordenamiento jurídico a nivel nacional, sino – y más importante – en el ámbito internacional. Un primer paso sería establecer unas reglas de juego en el ciberespacio. La reciente cumbre entre Biden y Putin podría presentar un rayo de esperanza hacia una posible y gradual cooperación en materia de seguridad cibernética (El País, 2021). Ya en septiembre de 2020, Putin manifestó en un comunicado oficial su interés de iniciar un diálogo, sosteniendo que "uno de los principales

retos estratégicos actuales es el riesgo de una confrontación a gran escala en el ámbito digital. Una responsabilidad especial para su prevención recae en los actores clave en el ámbito de la garantía de la seguridad de la información internacional (IIS). A este respecto, nos gustaría dirigirnos una vez más a los Estados Unidos con la sugerencia de acordar un programa global de medidas prácticas para reimpulsar nuestras relaciones en el ámbito de la seguridad en el uso de las tecnologías de la información y la comunicación (TIC)" (Presidente de Rusia, 2020). Sin embargo, de momento, EE. UU. se ha mostrado reacio a la hora de colaborar con Rusia en esta materia- queda por ver en qué se quedarán estas primeras conversaciones bilaterales algo difusas. También se han iniciado propuestas por parte de Gran Bretaña en la cumbre del G7 para crear un mecanismo de respuesta rápida a la "propaganda y desinformación rusa" (Reuters, 2021), entre otras cosas.

Por otro lado, y siguiendo las propuestas de Galán (2018), en el plano cultural, es esencial concienciar a la sociedad de esta amenaza a la que nos enfrentamos día a día para prevenir y mitigar los efectos de lo que Wardle y Derakhshan (2017) llaman el "desorden informacional" del siglo XXI.

Finalmente, a estos dos aspectos que propone Galán, añadiría la necesidad de formular una definición clara en el ámbito académico de cada uno de los conceptos que contengan el adjetivo "híbrido", "no lineal" o sus derivados (irregular, asimétrico, ambiguo), ya que la falta de uniformidad definitoria sólo da lugar a una amalgama de informes, artículos y demás publicaciones que en parte no logran captar la esencia de todo lo que llevan consigo tales conceptos. En especial, urgiría convergir las diferentes comprensiones – en parte incluso dispares– que tienen Occidente y Rusia de aquellos, para evitar que lo "híbrido" se convierta en un "concepto comodín" (Colom Piella, 2019, p.7).

Para concluir esta monografía, es necesario recordar que, evidentemente, el presente trabajo está lejos de ser completo y, – aunque se haya procurado evitar en la medida que es posible – por ende, en alguna ocasión se puede haber recurrido a simplificaciones.

## REFERENCIAS


Alliance for securing democracy (2021). *Authoritarian Interference Tracker*. https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/

Amann, M., Heffner, S., Knobbe, M., Müller, A.K., Puhl, J., Rosenbach, M., Sarovic, A., Schmitt, J., Wiedmann-Schmidt, W. y Zeller, A. (05/04/2019). Wie Wladimir Putin die AfD für seine Zwecke benutzt. *Der Spiegel*. https://www.spiegel.de/politik/wie-putin-die-afd-fuer-seine-zwecke-missbraucht-a-00000000-0002-0001-0000-000163279501

Andrew, C. (2001). *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. Basic Books, 1999, pp. 244–246

Antonov, M. (17/09/2017). PR-война: Мадрид и Барселона готовятся к генеральному сражению. *Vesti7*. https://vesti7.ru/article/678683/episode/17-09-2017/

Armistead, L .(2004). *Information operations: warfare and the hard realities of power*. Brassey´s Inc.

Asociación para la Investigación de Medios de Comunicación (AIMC). (2021). *Ranking de diarios*. https://reporting.aimc.es/index.html#/main/diarios

Barbashin, A.; Thoburn, H. (31/03/2014). Putin´s Brain. *Foreign Affairs*. https://www.foreignaffairs.com/articles/russia-fsu/2014-03-31/putins-brain

Baqués, J. (2015). El papel de Rusia en el conflicto de Ucrania: La guerra híbrida de las grandes potencias. *Revista de Estudios en Seguridad Internacional*, Vol. 1, No. 1 (2015), págs. 41-60. DOI: http://dx.doi.org/10.18847/1.1.3

BBC (29/11/2016). *German spy chief Kahl warns of election disruption.* http://www.bbc.com/news/world-europe-38142968

Bell, D. (1962). *The end of ideology: on the exhaustion of political ideas in the fifties*. Free Press

Beumers, B., Hutchings, S. C. y Rulyova, N. (2009). *The post-Soviet Russian media: Conflicting signals*. Routledge.

Bolgov R., Chernov I., Ivannikov I. y Katsy D. (2019). *Battle in Twitter: Comparative Analysis of Online Political Discourse (Cases of Macron, Trump, Putin, and Medvedev).* Communications in Computer and Information Science, vol 947. Springer, Cham. https://doi.org/10.1007/978-3-030-13283-5_28

Calderón Concha, Percy (2009). Teoría de conflictos de Johan Galtung. *Revista de Paz y Conflictos*, (2),60-81. https://www.redalyc.org/pdf/2050/205016389005.pdf

Calzini, P. (2005). Vladimir Putin and the Chechen war. *The International Spectator 40*(2): págs. 19–28. https://doi.org/10.1080/03932720508457122

Canal Uno. (23/10/2017). *Непокорная Каталония. Время покажет. Выпуск от 23.10.2017*. [Archivo de Video]. Youtube. https://www.youtube.com/watch?v=rjVJQo9Blxg&t=402s

Canal Uno. (08/10/2017*). Выпуск программы "Время" в 21:00, 8 октября 2017 года*. [Archivo de Video]. ПЕРВЫЙ КАНАЛ. https://www.1tv.ru/news/issue/2017-10-08/21:00#10

Centro Criptológico Nacional CCN (2018). Ciberamenazas y Tendencias. Edición 2018. *CCN-CERT IA 09/18. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenzas-y-tendencias-edicion-2018-1/file.html*

Chen, A. (2015). The Agency. *The New York Times Magazine*. https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Colás, X. (04/10/2017). La conexión moscovita del 'procés' con los hackers rusos. *El Mundo*. https://www.elmundo.es/cronica/2017/10/04/59cfd94ae5fdea54288b45d2.html

Colás, X. (05/02/2021). España cuestiona que Rusia sea una democracia tras comparar al opositor Alexei Navalny con los independentistas en España. *El Mundo*. https://www.elmundo.es/internacional/2021/02/05/601d33c1fc6c8364588b4674.html

Colom Piella, G. (2018). Guerras Híbridas. Cuando el contexto lo es todo. *Ejército: de tierra español*. Nº. 927 (diciembre), págs. 38-43. https://www.ugr.es/~gesi/Guerras-hibridas.pdf

Colom Piella, G. (2019). La amenaza híbrida: mitos, leyendas y realidades. *Documento de Opinión. IEEE 24/2019*. http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO24_2019GUICOL-hibrida.pdf

Colom Piella, G. (2020). Anatomía de la desinformación rusa. *Historia y comunicación social 25*(2), 473-480. https://doi.org/10.5209/hics.63373

Connel, M.; Vogler, S. (2016). Russia´s Approach to Cyber Warfare. *Center for Naval Analyses (CNA)*. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

Conley, H. A.; Mina, J.; Stefanov, R. y Vladimirov, M.(2016). *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe.* Center for Strategic and International Studies, https://www.csis.org/analysis/kremlin-playbook.

Deutsche Welle (DW) (02/05/2017). *Chancellor Merkel faces President Putin in tense Sochi press conference*. https://www.dw.com/en/chancellor-merkel-faces-president-putin-in-tense-sochi-press-conference/a-38664126

Deutsche Welle (DW) (04/07/2019). *Borrell no sitúa a Cataluña entre sus futuras funciones en Europa.* https://www.dw.com/es/borrell-no-sit%C3%BAa-a-catalu%C3%B1a-entre-sus-futuras-funciones-en-europa/a-49468801

Deutsche Welle (DW) (06/09/2020). Politicians in Germany warn ex-Chancellor Schröder to quit Russian posts. https://www.dw.com/en/gerhard-schröder-russia-germany/a-54829142

Diresta, R.; Shaffer, K.; Ruppel, B.; Sullivan, D.; Matney, R.; Fox, R.; Albright, J. y Johnson, B. (2018). The tactics & tropes of the Internet Research Agency. *New Knowledge*. https://digitalcommons.unl.edu/senatedocs/2/

Dixon, R. (01/04/2020). Trump called Russia's coronavirus aid to U.S. 'very nice.' Putin may use it as a propaganda coup. *The Washington Post.*

https://www.washingtonpost.com/world/europe/russia-coronavirus-aid-us-putin/2020/04/01/39d52cb2-7411-11ea-ad9b-254ec99993bc_story.html

Eckel, M. (06/05/2021). In U.S. Trial Of Alleged Hacker, Signs Of Larger Russian Cybercrimes. *Radio Free Europe/ Radio Liberty.* https://www.rferl.org/a/methbot-russia-internet-fraud-state-sponsored-hacking-zhukov/31241417.html

EEAS (2015). *Questions and Answers about the East StratCom Task Force*. https://eeas.europa.eu/headquearters/headquarter-Homepage/2116/questions-and-answers-about-east-stratcom-taskforce_en

EEAS (2018). *Action Plan Against Disinformation.* https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

Efe (2019). *Investigan si hay vínculos entre la inteligencia rusa y Tsunami Democràtic.* https://www.efe.com/efe/espana/politica/investigan-si-hay-vinculos-entre-la-inteligencia-rusa-y-tsunami-democratic/10002-4117144

Ejército de los EE. UU. (2011). *Field Manual (Manual de Operaciones) 3-0 Operations C-1*. https://www.globalsecurity.org/military/library/policy/army/fm/3-0/fm3-0_c1_2011.pdf

El País (17/06/2021). *EE UU-Rusia: reducir riesgos*. https://elpais.com/opinion/2021-06-17/ee-uu-rusia-reducir-riesgos.html

Elswah, M. y Howard, P.(2020). Anything that Causes Chaos: The Organizational Behavior of Russia Today (RT). *Journal of Communication*, *70*(5), Págs. 623-645. https://doi.org/10.1093/joc/jqaa027

Europa Press (13/11/2017). El Gobierno admite que la propaganda rusa ha influido en el conflicto catalán. *El Economista*. https://www.eleconomista.es/politica/noticias/8739685/11/17/Dastis-alerta-a-sus-socios-de-la-UE-de-que-la-propaganda-rusa-afecta-tambien-al-desarrollo-democratico-en-Cataluna.html

EUvsDisinfo (2020). Disinfo: RT is the voice of truth". EUvsDisinfo. https://euvsdisinfo.eu/report/rt-is-the-voice-of-the-truth/

Fontana, D. W. (2018). MASS Media y Conflictos Híbridos: el caso de la Guerra de la Información y la Revolución de Color. *IOSR Journal Of Humanities And Social Science (IOSR-JHSS)*. *23*(3), págs. 01-12. DOI: 10.9790/0837-2303070112

Galán, J., Abad Liñán, J.M. y Alameda, D. (04/12/2017). Los 4.800 bots que jalearon el 'procés'. *El País*. https://elpais.com/politica/2017/12/04/actualidad/1512389091_690459.html

Galán, C. (2018). Amenazas híbridas: nuevas herramientas para viejas aspiraciones. *Real Instituto Elcano*. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt20-2018-galan-amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones

Galeotti, M. (2014). The 'Gerasimov Doctrine' and Russian Non-Linear War. *In Moscow's Shadows*. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov- doctrine-and-russian-non-linear-war

Galeotti, M. (2015). "Hybrid War as a War on Governance" Interview by Octavian Manea. *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/hybrid-war-as-a-war-on-governance

Gallacher , J. D. y Heerdink, M.W. (2019). Measuring the Effect of Russian Internet Research Agency Information Operations in Online Conversations. *Defence Strategic Communications 6*. https://stratcomcoe.org/publications/measuring-the-effect-of-russian-internet-research-agency-information-operations-in-online-conversations/95

Galtung, J. (1996). *Peace by Peaceful Means: Peace and Conflict, Development and Civilization*. SAGE.

García, J. (28/10/2020). El juez investiga al círculo de Puigdemont por sus contactos con el Kremlin. *El País*. https://elpais.com/espana/catalunya/2020-10-28/el-juez-investiga-al-circulo-de-puigdemont-por-sus-contactos-con-el-kremlin.html

Generalbundesanwalt (2021). *Festnahme wegen mutmaßlicher geheimdienstlicher Agententätigkeit*. https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/aktuelle/Pressemitteilung-vom-21-06-2021.html

Giles, K. (2016). Handbook of Russian information warfare. *NATO Defence College*. https://www.ndc.nato.int/news/news.php?icode=995

Gioe, D.V., Lovering, R., y Pachesny, T.(2020). "The soviet legacy of Russian active measures: new vodka from old stills?". Int J Intell Counterintell;33: 1–26.https://www.tandfonline.com/doi/full/10.1080/08850607.2020.1725364

Gorodnichenko, Y., Pham, T. y Talavera, O. (2018). Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #USElection. *NBER Working Paper No. 24631*. DOI 10.3386/w24631

Grant, N. (1990). Security and the Soviet Émigré Problem: Hoods and Spies in 'The Big Candy Store'. *Conservative Review*. https://oac.cdlib.org/findaid/ark:/13030/kt1r29q8hs/dsc/

Grinda González, J. (2015). Regulación nacional e internacional del crimen organizado. Experiencia de la Fiscalía Anticorrupción. *Fiscalía General del Estado.* https://www.fiscal.es/documents/20142/172963/INFOFISCALIA_MAYO_09.pdf/8fea8dae-df01-ea69-ad93-472d5766cb80?version=1.0&t=1537196293679

Grynszpan, E. (11/07/2014). Andreï Zoubov: «Poutine crée un manuel d'histoire qui répond aux attentes des Russes». *Le Temps*. https://www.letemps.ch/culture/andrei-zoubov-poutine-cree-un-manuel-dhistoire-repond-aux-attentes-russes

Hauteville, J. M. (30/05/2018). Russia trip exposes AfD ties to Moskow. *Handelsblatt*. https://www.handelsblatt.com/english/politics/russian-collusion-russia-trip-exposes-afd-ties-to-moscow/23582296.html?ticket=ST-32090-ogEf5fIPYWdC7PBUjAmx-ap6

Higgins, A. (2019). The War That Continues to Shape Russia, 25 Years Later. *The New York Times.* https://www.nytimes.com/2019/12/10/world/europe/photos-chechen-war-russia.html

Hulcoop, A., Scott-Railton, J., Tanchak, P., Brooks, M. y Deibert. R. (2017). Tainted Leaks: Disinformation and Phishing with a Russian Nexus. *Citizen Lab Research Report No. 92*, University of Toronto. https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

Instituto Internacional de Investigación para la Paz de Estocolmo (SIPRI) (2021). Data for all countries from 1988–2020 as a share of GDP. *Yearbook: Armaments, Disarmament and International Security.* https://sipri.org/sites/default/files/Data%20for%20all%20countries%20from%201988–2020%20as%20a%20share%20of%20GDP%20%28pdf%29.pdf

Iosifidis, P., y Wheeler, M. (2018). Modern political communication and web 2.0 in representative democracies. *Javnost-The public, 25*(1-2), págs. 110-118. https://doi.org/10.1080/13183222.2018.1418962

Jensen, B., Valeriano, B. y Maness, R. (2019): Fancy bears and digital trolls: Cyber strategy with a Russian twist, *Journal of Strategic Studies*. http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/fancy_bears_and_digital_trolls_cyber_strategy_with_a_russian_twist_-_jss.pdf

Joseph, J. (2014). Realism and Neorealism in International Relations Theory. *The Encyclopedia of Political Thought*, M.T. Gibbons. (Ed.). https://doi.org/10.1002/9781118474396.wbept0864

Kofman, M. y Rojansky, M. (2015). A Closer Look at Russia's 'Hybrid War,'. *Kennan Institute*. http://www.isn.ethz.ch/Digital- Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24- a6a8c7060233&lng=en&id=190090

Laborde, A. (27/12/2020). Anatomía del gran ciberataque que ha comprometido el corazón de la Administración de EE..UU.. *El País*. https://elpais.com/internacional/2020-12-27/anatomia-del-gran-hackeo-que-ha-comprometido-el-corazon-de-la-administracion-de-eeuu.html

Laborde, A. (14/12/2020). Estados Unidos sospecha que Rusia está detrás de un pirateo informático a agencias federales. *El País*. https://elpais.com/internacional/elecciones-usa/2020-12-14/estados-unidos-sospecha-de-rusia-como-responsable-del-pirateo-a-agencias-federales.html

Laborde, A. (23/02/2021). EE. UU. prepara sanciones contra Rusia por el ciberataque masivo a agencias federales y el 'caso Navalni'. *El País*. https://elpais.com/internacional/2021-02-23/ee-uu-prepara-sanciones-contra-rusia-por-el-ciberataque-masivo-a-agencias-federales-y-el-caso-navalni.html

Lafer, C. (2002). *La identidad Internacional de Brasil*, Buenos Aires, Fondo de Cultura Económica.

Lesaca, J. (22/11/2017).Why did Russian social media swarm the digital conversation about Catalan independence? *The Washington Post*. https://www.washingtonpost.com/news/monkey-cage/wp/2017/11/22/why-did-russian-social-media-swarm-the-digital-conversation-about-catalan-independence/

LISA Institute (2019). *Qué es la Guerra Híbrida y cómo nos afectan las Amenazas Híbridas.* https://www.lisainstitute.com/blogs/blog/guerra-hibrida-amenazas-hibridas

Lo, B. (2018). Chutzpah and Realism: Vladimir Putin and the Making of Russian Foreign Policy. *Russie.Nei.Visions, No. 108, Ifri*. https://www.ifri.org/sites/default/files/atoms/files/bobo_lo_chutzpah_and_realism_2018.pdf

López- Fonseca, Ó. (17/05/2021). La Audiencia Nacional archiva la investigación sobre la presencia de espías rusos en Cataluña durante el 'procés'. *El País*. https://elpais.com/espana/2021-05-17/la-audiencia-nacional-archiva-la-investigacion-sobre-la-presencia-de-espias-rusos-en-cataluna-durante-el-proces.html

López Jiménez, J. E. (2019). Fake News, Munición de guerra. *Revista Ejército de tierra español*. ISSN 1696-7178, Nº. 945 (Diciembre), págs. 10-13. https://ejercito.defensa.gob.es/Galerias/multimedia/revista-ejercito/2019/945/accesible/Revista_Ejercito_Accesible.pdf

López-Olano, C. y Fenoll, V. (2019). Posverdad, o la narración del procés catalán desde el exterior: BBC, DW y RT. *El profesional de la información*, v. 28, n. 3. https://doi.org/10.3145/epi.2019.may.18

Marraco, M. (21/11/2019). La Audiencia Nacional sigue el rastro de un espía ruso que estuvo en Cataluña justo antes del 1-O. *El Mundo*. https://www.elmundo.es/espana/2019/11/21/5dd66bb721efa0e9708b45e1.html

Martens, B., Aguiar, L., Gómez, M. y Muller-Langer, F. (2018). The digital transformation of news media and the rise of disinformation and fake news. *Joint Research Centre Unión Europea*. https://ec.europa.eu/jrc/communities/sites/jrccties/files/dewp_201802_digital_transformation_of_news_media_and_the_rise_of_fake_news_final_180418.pdf

Martín Serrano, L. F. (2020). El Ártico. La gran baza rusa (I). *Atalayar*. https://atalayar.com/content/el-ártico-la-gran-baza-rusa-i

McGrath, M. C. (2018). *Written evidence submitted to Parliament UK*. https://cutt.ly/BlMtY5

Medvedev, S. (2015). *Offense-defense theory analysis of Russian cyber capability* [Disertación doctoral, Naval Postgraduate School]. The NPS Theses and Dissertations. Institutional Archive. https://calhoun.nps.edu/handle/10945/45225

Milosevich-Juaristi, M. (2017). El poder de la influencia rusa: la desinformación. *Real Instituto Elcano*. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari7-2017-milosevichjuaristi-poder-influencia-rusa-desinformacion

Milosevich-Juaristi, M. (2017). La "combinación", instrumento de la guerra de la información de Rusia en Cataluña. *Real Instituto Elcano*. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari86-2017-milosevichjuaristi-combinacion-instrumento-guerra-informacion-rusia-cataluna

Ministerio del Interior Alemán (2015). *Informe sobre la protección de la Constitución*. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2016/06/vorstellung-verfassungsschutzbericht-2015.html

Morales, S. (2015). Herramientas de modificación y ampliación del área de influencia estratégica de Rusia, *Revista de Estudios en Seguridad Internacional*, Vol. 1, No. 2, pp. 85-107. DOI: http://dx.doi.org/10.18847/1.2.4

Murray, W. y Mansoor, P. R. (2012). *Hybrid Warfare. Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press.

National Intelligence Council (2017). Assessing Russian Activities and Intentions in Recent US Elections. *Government Printing Office*. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Nye, J. S. (2014). Putin's Rules of Attraction. *World Finance.* https://www.worldfinance.com/home/putins-rules-of-attraction

Ó Beacháin, D. y Polese, A. (2012). The Colour Revolutions in the Former Soviet Republics. *Successes and Failures. Routledge.*

Pardo de Santayana, J. (2017). Federación Rusa y yihadismo radical. Documento de Análisis. *Boletín IEEE*. Págs. 423-441. http://www.ieee.es/Galerias/fichero/docs_analisis/2017/DIEEEA56-2017_Rusia_y_yihad_JMPSGO.pdf

Parera, B. (11/02/2018). La Fiscalía no cree al antiguo Govern: busca saber cuántos heridos hubo de verdad el 1-O. *El Confidencial*. https://www.elconfidencial.com/espana/cataluna/2018-02-11/fiscalia-general-cargas-referendum-1-o-heridos_1518718/

Pascual de la Parte, F. (2019). Sin la guerra en Ucrania no habría habido intervención rusa en Siria/ entrevistado por Vitaliy Stepanyuk. *Global Affairs*, Universidad de Navarra. https://www.unav.edu/web/global-affairs/detalle/-/blogs/-sin-la-guerra-en-ucrania-no-habria-habido-intervencion-rusa-en-siria-

Pawlak, P. (2017). Countering hybrid threats: EU-NATO cooperation. *EPRS European Parliamentary Research Service.* *https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf*

Pintado Rodríguez, C. (2017). Ucrania. Un Estudio de Caso de Guerra Híbrida. *CISDE*. https://observatorio.cisde.es/actualidad/ucrania-un-estudio-de-caso-de-guerra-hibrida/

Posetti, J. y Matthews, A (2018): Una Breve Guía de la Historia de las "Noticias Falsas" y la Desinformación: Un Nuevo Módulo de Aprendizaje. *International Center for Journalists.* https://www.icfj.org/sites/default/files/2019-06/HistoryPropaganda_Espanol2_final_5.pdf

Presidente de Rusia (2020). *Statement by President of Russia Vladimir Putin on a comprehensive program of measures for restoring the Russia – US cooperation in the field of international information security*. http://en.kremlin.ru/events/president/news/64086

Rakuszitzky, M. (2019). Third Suspect in Skripal Poisoning Identified as Denis Sergeev, High-Ranking GRU Officer. *Bellingcat*. https://www.bellingcat.com/news/uk-and-europe/2019/02/14/third-suspect-in-skripal-poisoning-identified-as-denis-sergeev-high-ranking-gru-officer/

Rid, T. (2020). *Active measures: the secret history of disinformation and political warfare* (First edition.).

Rodríguez García, A. (10/02/2021). Los propios abusos que la UE (y España) obvia cuando habla de derechos humanos a Rusia. *RT*. https://actualidad.rt.com/opinion/alberto-rodriguez-garcia/383088-abusos-ue-espana-obviar-derechos-humanos-rusia

Roman, N., Wanta, W., y Buniak, I. (2017). Information wars: Eastern Ukraine military conflict coverage in the Russian, Ukrainian and U.S. newscasts. *International Communication Gazette*, 79(4), 357–378. https://doi.org/10.1177/1748048516682138

Romerstein, H. (2001). Disinformation as a KGB Weapon in the Cold War, *Journal of Intelligence History*, Vol. 1, No. 1, pp. 54–67. https://doi.org/10.1080/16161262.2001.10555046

*RT*. (21/11/2017). La inteligencia española descarta ciberataques del Gobierno ruso durante la crisis catalana. https://actualidad.rt.com/actualidad/255746-inteligencia-espanola-descarta-ciberataques-rusia?utm_source=rt_app&utm_medium=app&utm_campaign=links_app

RT France. (19 enero 2019). *Laurent Dauré : «Les accusations de fake news c'est un outil politique pour intimider»*. [Archivo de Video]. Youtube. https://www.youtube.com/watch?v=AfNvjK8Jfrs

RT France. (23 octubre 2020). *Les méchants russes*. [Archivo de Video]. Youtube. https://www.youtube.com/watch?v=j9FCX-Voc6Y

Ruiz González, F. J. (2013). *El Concepto de Política Exterior de Rusia: un estudio comparado*. http://www.ieee.es/Galerias/fichero/docs_marco/2013/DIEEEM06-2013_Rusia_ConceptoPoliticaExterior_FRuizGlez.pdf

Rumsfeld, D. (2005). The National Defense Strategy of the United States of America. *U.S. Department of Defense*. https://archive.defense.gov/news/Mar2005/d20050318nds1.pdf

Sabrodin, A. (28/09/2016). Каталония признает Крым российской территорией. *Izvestia*. https://iz.ru/news/634567

San Martín, H. (2019). *La Guerra Híbrida Rusa Sobre Occidente*. Page Publishing Inc. (Primera edición).

Schick, N. (29/01/2021). Deepfakes Q&A with Nina Schick part 1: Misinformation and the origins of deepfakes. *Faculty*. https://faculty.ai/blog/deepfakes-qa-with-nina-schick/

Schreiber, W. (2016). DER NEUE UNSICHTBARE KRIEG? Zum Begriff der „hybriden" Kriegführung. *Aus Politik und Zeitgeschichte: Moderne Kriegsfuehrung. Zeitschrift der Bundeszentrale fuer politische Bildung.* 35–36/2016. Págs. 11-15.

Schwirtz, M. (08/10/2019). Top Secret Russian Unit Seeks to Destabilize Europe, Security Officials Say. *New York Times*. https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html

Schultz, R. y Godson, R. (1984). *Desinformatsia*. Pergamon Brassey's,

Scocozza, C. (2017). Una aproximación rusa al poder blando en el actual sistema internacional. *OASIS*, 25, 63-74. DOI: https://doi.org/10.18601/16577558.n25.04

Segura, C. (26/09/2017). Assange alienta que la rebelión en Cataluña se extienda a nivel global. *El País.* https://elpais.com/ccaa/2017/09/26/catalunya/1506456387_836185.html

Select Committee on Intelligence (2018). *Report on Russian active measures*, House of Representatives. https://www.congress.gov/115/crpt/hrpt1110/CRPT-115hrpt1110.pdf

Shalal, A. (04/05/2017). Germany challenges Russia over alleged cyberattacks. *Reuters*. https://www.reuters.com/article/us-germany-security-cyber-russia-idUSKBN1801CA

Shalal, A. y Auchard, E. (22/09/2017). German election campaign largely unaffected by fake news or bots. *Reuters*. www.reuters.com/article/us-germany-election-fake/german-election-campaign-largely-unaffected-by-fake-news-or-bots-idUSKCN1BX258

Shuster, S. (09/08/2017). Russia Has Launched a Fake News War on Europe. Now Germany Is Fighting Back, *TIME*. http://time.com/4889471/germany-election-russia-fake-news-angela-merkel/

Smith, D. (2011). Democracy, Democratisation and Peace – Lessons from Recent Experience. *FriEnt, 8*. https://d-nb.info/1045375349/34

Sputnik. (21/09/2017). *El independentismo: una bomba de relojería contagiosa en un Estado que no escucha*. https://mundo.sputniknews.com/20170921/independentismo-mallorca-consecuencias-1072539400.html

Sputnik. (08/02/2021). *La UE niega comparaciones entre Navalni y los líderes del independentismo catalán*. https://mundo.sputniknews.com/20210208/la-ue-niega-comparaciones-entre-navalni-y-los-lideres-del-independentismo-catalan-1094363082.html

Stake, R. (1995*). The art of case research*. Sage Publications.

Stelzenmüller, C. (2017). The Impact of Russian Interference on Germany's 2017 Elections. *Robert Bosch Senior Fellow, Center on the United States and Europe Brookings Institution*. https://www.bosch-stiftung.de/sites/default/files/documents/downloads/Stelzenmueller_Brookings_Russian_influence_SSCI_Testimony.pdf

Sumantra, M. (2015). Was Putin Ever a Friend of the West? Realism and the Rise and Decline of Putin's Rapprochement with the Bush Administration after 9/11. *JIR*. http://dx.doi.org/10.2139/ssrn.2704623

Telman Sánchez Ramírez, P. T. (2009). La actual política exterior de la Federación Rusa. Una mirada desde el realismo político. *Revista Enfoques*, VOL VII, Nº 10, p.269. http://www.revistaenfoques.cl/index.php/revista-uno/article/view/192

Telman Sánchez Ramírez, P. T. (2010). La Federación Rusa y su entorno geopolítico en los nuevos arreglos mundiales de poder. *Política y cultura*, (34), 159-185. https://www.redalyc.org/pdf/267/26715367008.pdf

Terrasa, R. (15/10/2019). Qué es Tsunami Democràtic: manual para la rebelión independentista en tiempos de WhatsApp. *El Mundo*. https://www.elmundo.es/cataluna/2019/10/15/5da5b523fdddfffa3a8b45c0.html

*The Economist* (14/02/2015). In the Kremlin's pocket. Who backs Putin and why. https://www.economist.com/briefing/2015/02/12/in-the-kremlins-pocket

Thomas, T. L. (2001) Information Security Thinking: A Comparison of U.S., Russian, And Chinese Concepts. *Foreign Military Studies Office*. https://doi.org/10.1142/9789812776945_0032

Thornton, R. (2015). The Changing Nature of Modern Warfare: Responding to Russian Information Warfare. *RUSI Journal* 160, 4:40-48. ttps://doi.org/10.1080/03071847.2015.1079047

U.S. Department of Justice (2018). *United States of America v. Internet Research Agency, et al.* Caso 1:18-cr-00032-DLF. https://www.justice.gov/file/1035477/download

Vacas Fernández, F. y Calvo Albero, J.L. (2005). El Conflicto de Chechenia. *Conflictos Internacionales Contemporáneos*. Ministerio de Defensa. https://publicaciones.defensa.gob.es/media/downloadable/files/links/e/l/el_conflicto_de_chechenia.pdf

Volkoff, V. (comp.) (1986). *La désinformation, arme de guerre*. Julliard.

Waltz, K. N. (1979*). Theory of international politics*. Addison-Wesley Pub. Co.

Wardle, C. y Derakhshan, H. (2017). Information Disorder: Towards an Interdisciplinary Framework for Research and Policy-Making, *Council of Europe*. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html#

Yablokov, I. (2015). Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT). *Politics*, *35*(3), págs. 301–315. https://doi.org/10.1111/1467-9256.12097

Yin, R. (1993*). Applications of case study research.* Sage Publishing.

Zubelzú, G. (2007). Entender a Rusia a través de sus fuerzas profundas: dificultades y desafíos de una reflexión recurrente. *Revista Brasileira de Política Internacional*, *50*(1), págs. 102-120. https://doi.org/10.1590/S0034-73292007000100006

Zygar, M. (2016). *All the Kremlin's Men: Inside the Court of Vladimir Putin*. New York, NY: PublicAffairs