ARTÍCULOS

Historia y comunicación social
ISSN: 1137-0734

EDICIONES COMPLUTENSE

http://dx.doi.org/10.5209/hics.63373

Anatomía de la desinformación rusa[1]

Guillem Colom Piella[2]

Recibido: 29 de enero de 19 / Aceptado: 10 de diciembre de 2019

Resumen. Advertida con sorpresa durante la invasión de Crimea y popularizada tras las pasadas elecciones presidenciales estadounidenses, la desinformación rusa está en boga. Sin embargo, estas actividades que combinan desinformación, propaganda, manipulación y falsificación documental utilizando medios abiertos, semi-encubiertos o clandestinos no son nuevas. Moscú concibió estas técnicas tras la revolución rusa, las utilizó durante la Guerra Fría y parece haberlas adaptado con gran éxito al mundo virtual. El artículo estudia sus componentes y subraya la continuidad que existe en sus tácticas, técnicas y procedimientos.
Palabras clave: Desinformación; medidas activas; Rusia; propaganda; operaciones de influencia.

[en] The anatomy of Russian disinformation

Abstract. Revealed with the invasion of Crimea and popularized after the 2016 U.S. presidential elections, Russian disinformation is in vogue. However, these activities that combine disinformation, propaganda, manipulation and forgeries using open, semi-concealed or clandestine means are not new. These techniques were conceived after the Soviet revolution, they were employed during the Cold War and they have been successfully adapted to the virtual environment. The article studies its components and emphasizes the continuity that exists in its tactics, techniques and procedures.
Keywords: Disinformation; active measures; information warfare; Russia; propaganda; influence operations.

Cómo citar: Colom Piella, G. (2020). Anatomía de la desinformación rusa. *Historia y comunicación social* 25(2), 473-480.

1. Introducción

Advertida con sorpresa durante la invasión de Crimea y popularizada tras los pasados comicios presidenciales estadounidenses, la desinformación rusa se ha puesto de moda. Se cita en discursos gubernamentales de muchos países de nuestro entorno y se percibe con preocupación por la Unión Europea o la Alianza Atlántica. Sin embargo, la difusión de información falsa o engañosa usando medios abiertos, semi-encubiertos o clandestinos no es nueva. Moscú concibió estas técnicas durante el régimen zarista, las codificó tras la revolución rusa, las utilizó durante la Guerra Fría y las ha adaptado con enorme éxito al mundo virtual. Aunque popularmente se las defina como "desinformación", estas actividades que combinan desinformación con propaganda, manipulación o falsificación documental son formalmente denominadas "medidas activas".

Este trabajo estudiará las medidas activas rusas en el exterior. Estas actividades han sido empleadas por Moscú de forma casi ininterrumpida desde hace más de un siglo para apoyar las labores de propaganda, influencia, subversión y desestabilización. Para ello, el artículo definirá algunos conceptos clave, repasará la evolución y características de la desinformación durante la Guerra Fría y debatirá sobre su migración al mundo online o la continuidad existente en las tácticas, técnicas y procedimientos utilizados antes y ahora. Aunque se combinarán fuentes primarias y secundarias, ante la escasez de documentación oficial rusa en abierto, el dinamismo del objeto de estudio y la aparente desconexión que existe entre los estudiosos de la desinformación y los analistas en asuntos militares, varias ideas se fundamentarán en fuentes occidentales, lecciones identificadas de casos recientes y especulaciones en base al nutrido debate militar ruso en materia de guerra informativa, un elemento de gran relevancia pero que escapa al objeto de este estudio.

[1] Este artículo ha sido realizado en el marco del proyecto "Ciberataques y gobernanza global" (DER2017-85612-R), financiado por el Ministerio de Economía, industria y competitividad (2018-21).
[2] Universidad Pablo de Olavide, Sevilla.
gcolpie@upo.es

2. Las medidas activas tradicionales

Las actividades de Moscú en su vecindad inmediata, en Crimea, Siria o el este de Ucrania o en procesos políticos occidentales han puesto de moda la desinformación rusa[3]. Aunque muchos la consideran como algo novedoso por la eficaz explotación de internet, ésta tiene un largo historial cuyos orígenes se remontan a las actividades de la policía secreta zarista (s. XIX)[4] y la Checa comunista (1917). Aunque continúa rodeada de un halo de misterio por la dificultad de acceder a fuentes primarias, la interesada imprecisión terminológica y la necesidad de fundamentar los análisis en las declaraciones de sus responsables o en fuentes secundarias, la desinformación contemporánea arrancó con la Tercera Internacional (1919) para apoyar la subversión comunista. Cuatro años después, el Comisariado del Pueblo para Asuntos Internos (NKVD) creó una oficina específica para coordinar la desinformación soviética, un conjunto de actividades que englobaban – tal y como había puesto en práctica la Ojrana zarista décadas atrás – la distorsión de hechos y la propagación de rumores. Definida por el KGB como "…la invención de datos para generar, en la mente del adversario, imágenes incorrectas o imaginarias de la realidad para que éste tome decisiones beneficiosas [para Moscú]" (KGB, 1972: 79), la desinformación se distinguía de la propaganda política por su origen encubierto y difusión clandestina.

Con el inicio de la Guerra Fría, el KGB creó el departamento D (*desinformatsiya*) para organizar la desinformación, en coordinación con el Departamento Internacional del Partido Comunista y bajo la autoridad del Politburó (U.S. Department of State, 1981). Sin embargo, en la década de 1960 esta unidad dependiente del primer directorado de la KGB – encargado de las operaciones en el exterior – se transformó en el departamento A (*aktivnyye meropriyatiya* o medidas activas) para confundir a la inteligencia estadounidense sobre sus actividades reales (Jones, 2018). Definidas por el KGB como "…labores para influir sobre la vida política del país objetivo […] engañando al adversario, erosionando y debilitando sus posiciones, rompiendo sus planes hostiles o logrando otros fines" (Mitrokhin, 2002: 13)[5], las medidas activas aparentemente comprendían una amplia gama de operaciones de influencia para apoyar la subversión y desestabilización de los enemigos de Moscú (Romerstein, 1990)[6]. Fue en aquel momento cuando Washington adoptó esta idea que había sido utilizada por primera vez en el Komintern (1919) para describir cualquier actividad de influencia encaminada a reforzar la posición soviética y erosionar la imagen occidental (Kux, 1985). Desde entonces, ambas ideas se han utilizado como sinónimos[7], si bien Moscú continuó priorizando el término desinformación y Washington el de medidas activas, quizás para subrayar su peligrosidad como forma de guerra política (Godson y Shultz, 1985)[8]. Hoy en día, Estados Unidos ha vuelto a utilizar este término, tal y como indican todos los documentos oficiales elaborados a raíz del intento ruso de influir en los comicios presidenciales de 2016.

Las medidas activas podían realizarse de forma abierta, semi-encubierta o clandestina combinando desinformación con propaganda, manipulación de medios (insertando noticias falsas) y fabricación de información (falsificando fuentes). También podían usar medios clandestinos para diseminar información falsa, *proxies* (partidos, sindicatos o asociaciones con acreditados vínculos con Moscú), organizaciones pantalla (entidades científicas, culturales o pacifistas sin aparente relación con la URSS), agentes de influencia (que usarían su posición pública para apoyar secretamente al Kremlin), manipulación económica, chantaje (*kompromat*) o colaboradores que apoyarían consciente o inconscientemente la narrativa soviética (Kux, 1985; Shultz; Godson, 1984). Otras fuentes sostenían que las medidas activas también podían implicar secuestros, asesinatos, sabotajes o actos terroristas (Andrew y Mitrokhin, 2000; Bittman, 1985)[9], aunque este tipo de actividades encubiertas no se tratarán en este trabajo. Tal y como se observará en las próximas páginas, estos mismos vectores continuarán utilizándose hoy en día para desinformar, confundir e influir al adversario, adaptando las tácticas, técnicas y procedimientos para operar en el entorno online.

---

3 Para una visión panorámica del concepto, véase Rodríguez (2018). Sin embargo, quizás sería necesario contextualizar su empleo tradicional en las zonas grises bajo el umbral del conflicto armado, más que como "arma" de guerra.

4 Quizás, la *fake news* más famosa de la Ojrana zarista fue la obra "Los protocolos de los sabios de Sion". Publicado en 1902 para justificar los pogromos contra los judíos, en la actualidad este documento continúa siendo referenciado por numerosos conspiracionistas para justificar su antisemitismo. Tras la revolución de octubre, la Checa soviética sucedió a la Ojrana, de la que asimiló su organización.

5 Paradójicamente, el diccionario de contrainteligencia propone otra definición complementaria bajo el epígrafe M (*meropriyatiya aktivnyye)*: *"…actos de contrainteligencia que permiten penetrar en las intenciones del adversario, anticipándose a sus acciones, induciéndole a errores, negándole la iniciativa o frustrando sus acciones de sabotaje."* (KGB, 1972: 161).

6 Ello derivaría de las declaraciones del desertor Yuri Bezmenov, que equiparaba las medidas activas con el modelo de subversión ideológica del KGB. Dividida en cuatro fases, ésta empezaría con la desmoralización (negando evidencias y planteando realidades alternativas) y la desestabilización (debilitando los pilares del estado, la economía y la sociedad) antes de culminar con la crisis y la normalización bajo control socialista (Bezmenov, 1984). Este planteamiento parece coherente con algunos de los objetivos acreditados – como la alteración de la percepción de la realidad, la polarización social o la erosión de la confianza entre la ciudadanía y sus instituciones – de las medidas activas. Ideas similares han resurgido entre la comunidad de expertos rusa con los debates sobre guerra informativa, las guerras de nueva generación o las medidas no-militares para la resolución de conflictos (Gerasimov, 2013).

7 En este sentido, son muy representativas las palabras del coronel Rolf Wagenbreth, director del departamento X (desinformación) de la inteligencia exterior de Alemania Oriental, cuando declaró que: "Our friends in Moscow call it 'dezinformatsiya.' Our enemies in America call it 'active measures,' and I, dear friends, call it 'my favorite pastime." (citado en Boghardt, 2009: 1). Paradójicamente, hoy en día muchos servicios de información del antiguo bloque oriental utilizan el término medidas activas para referirse a las actividades de influencia y desestabilización rusas.

8 En términos generales, la guerra política se refiere al uso de todas las herramientas al servicio del estado – económicas, políticas, informativas, diplomáticas o militares – para desestabilizar otro estado sin cruzar el umbral del conflicto armado.

9 Recientemente se ha observado un repunte de estas operaciones – como el envenenamiento del matrimonio Skripal – concurrentes con el repunte de las operaciones de inteligencia agresivas y las medidas activas contra occidente, lo que podría sugerir la continuidad que existe entre esta gama de actividades de subversión y desestabilización susceptibles de ser utilizadas en la amplia zona gris que existe entre la paz y las hostilidades abiertas.

Aunque desde entonces las medidas activas y la desinformación se han utilizado como sinónimos, en sentido estricto las primeras parecían diferir de la desinformación porque integraban la propaganda blanca y usaban mayor variedad de actores, vectores y herramientas para diseminarla (Shultz y Godson, 1984). En cualquier caso, ambas tácticas pretendían manipular las percepciones de su ciudadanía para mejorar la aceptación de las acciones soviéticas, erosionar las relaciones diplomáticas entre aliados, polarizar la sociedad y su confianza en las instituciones políticas o lograr el "control reflexivo" sobre sus líderes políticos manipulando su proceso de toma de decisiones para beneficiar a Rusia (Giles, 2016; Andrew y Mitrokhin, 2000)[10].

Durante la Guerra Fría, Moscú dedicó importantes recursos a estas actividades para exponer las bondades del socialismo y las contradicciones de occidente. Segmentadas para alcanzar distintas audiencias y ajustadas al país objetivo para explotar sus clivajes sociales, las medidas activas comprendían desde asuntos plausibles (las tensiones raciales en Estados Unidos, la herencia del nazismo en Alemania, el neocolonialismo en el tercer mundo o el atlantismo en España)[11] a los más rocambolescos (el arma que distinguía entre blancos y negros, la falsa llegada a la Luna, contactos con extraterrestres o la creación del SIDA en un laboratorio) (Abrams, 2016; Boghardt, 2009; Andrew; Mitrokhin, 2000; Kux, 1985; Bittman, 1985). Sin embargo, los temas predilectos se relacionaban con las armas atómicas, la política exterior estadounidense o el riesgo de desatarse una guerra en Europa para movilizar a grupos antiestadounidenses, pacifistas y antinucleares y explotar los miedos de las sociedades occidentales, erosionar la cohesión aliada y forzar cambios en su estrategia militar (U.S. Senate, 1985).

Se especula que, durante este periodo histórico, el KGB dedicó hasta el 80% de sus medios humanos y materiales a las medidas activas (Andrew; Mitrokhin, 2000), desconociéndose cuántos de ellos se utilizaron para manipular medios de comunicación. Sin embargo, fuentes de la época estiman que su impacto fue limitado porque no influyeron sobre la opinión pública ni en las decisiones políticas occidentales (Kux, 1985). De poco servía que plataformas comunistas o clandestinas diseminaran la desinformación y que medios sensacionalistas la replicaran. Aunque varios rumores y conspiraciones – desde el origen del SIDA (Boghardt, 2009) a la campaña contra el despliegue de los *euromisiles* (Wettig, 2009)[12] – lograron cierta popularidad, para ocultar su procedencia, dificultar su atribución, dotarla de legitimidad y llegar al gran público era necesario insertar la desinformación en los principales medios de comunicación occidentales (U.S. Department of State, 1981). Sin embargo, aunque los denominados "agentes de influencia" – periodistas, activistas, académicos o líderes de opinión – podían utilizar distintas técnicas para intentar influir sobre la población, el ecosistema mediático existente (más reducido, con mayores medios humanos, materiales o económicos y menos sujeto a la inmediatez) o la verificación de las fuentes y de los documentos filtrados a la prensa permitían limitar la desinformación. No obstante, estudios más recientes concluyen que la infiltración en los movimientos pacifistas y organizaciones científicas o la explotación occidental del miedo a una guerra (coincidiendo con el despliegue de los "euromisiles" o la "guerra de las galaxias") (Colom, 2018) no alteró muchas decisiones políticas, pero sí influyó sobre la opinión pública (Jones, 2018; Wettig, 2009).

Aunque se tiende a asumir que las medidas activas acabaron con el fin de la Guerra Fría y se retomaron tras el acceso de Vladimir Putin a la presidencia de la Federación Rusa (Darczewska; Żochowski, 2018), lo cierto es que entre 1989 y 1992 Moscú utilizó tácticas similares para alentar en occidente los temores sobre los efectos que la disolución de la URSS podría tener sobre la estabilidad global (U.S. Information Agency, 1992). Y en la segunda mitad de la década, los servicios de información de muchos países del área de influencia directa de Moscú detectaron actividades encaminadas a "…influir en las decisiones de los gobiernos locales, diseminar información falsa, erosionar la credibilidad del país en el extranjero y minar la confianza de la ciudadanía hacia sus autoridades" (Security Information Service [BIS], 1997, citado en Bugajski, 2004: 160). Sin embargo, fue necesario esperar hasta 2008 para la inteligencia checa fuera la primera en declarar públicamente que el Kremlin había retomado "…la práctica soviética de utilizar medidas activas para promover sus intereses de política exterior" (BIS, 2009: 5). Sin embargo, fue necesario esperar a los sucesos de Ucrania y los comicios presidenciales estadounidenses para que estas tácticas volvieran a popularizarse.

3. Las medidas activas en la actualidad

Aunque apenas han cambiado en su concepción, las medidas activas contemporáneas han multiplicado su alcance explotando las posibilidades que brinda internet. Han adaptado sus tácticas e instrumentos al mundo digital, adoptado vectores y lenguajes propios de este dominio, aprovechado las debilidades de las sociedades avanzadas para diluir

---

[10] Definido como "…el proceso por el cual un enemigo transmite a otro las razones o bases para su toma de decisiones" (Lefevre, citado en Thomas, 2004: 244), el control reflexivo empezó a desarrollarse en la década de 1960 para explicar los mecanismos psicológicos que permitirían manipular el proceso decisorio del adversario. Aunque trasciende al ámbito militar, sus antecedentes se hallan en la *maskirokvka* militar, que utilizaba una amplia gama de técnicas (camuflaje, ocultación, seguridad operativa, desinformación, engaño, diversión o estratagemas) para confundir al adversario en los niveles táctico y operacional de la guerra.

[11] En noviembre de 1981, semanas antes de formalizar la solicitud de ingreso, se filtró sin éxito a la prensa española una carta falsificada del presidente Reagan que instaba al rey Juan Carlos I a forzar la entrada del país en la OTAN y tomar medidas contra el Opus Dei y los partidos de izquierdas (Departament of State, 1982: 1-2).

[12] No obstante, téngase en cuenta que, a diferencia de otras campañas que utilizaban el argumento pacifista, ésta también partía de un miedo que el Kremlin consideraba real: la posibilidad de que Estados Unidos desplegara estos misiles para posibilitar un ataque de decapitación contra el liderazgo soviético (Colom, 2018).

la línea entre los hechos y la ficción o utilizado la libertad de expresión para introducir contenido extremista. A diferencia del pasado, las medidas activas tampoco pretenden convencer de las bondades del sistema político ruso, sino explotar la desafección política, el relativismo, las actitudes posmodernas o las contradicciones occidentales para desacreditar sus políticas, polarizar a sus poblaciones, manipular sus procesos de toma de decisiones o proyectar los intereses rusos (Helmus *et al.*, 2018; Polyakova; Boyer, 2018; Giles, 2016).

Precisamente, el potencial de las nuevas tecnologías para influir sobre las opiniones públicas y desestabilizar gobiernos ha sido un asunto recurrente en la comunidad de inteligencia rusa desde el fin de la Guerra Fría (Soldatov; Borogan, 2015)[13]. Estos miedos se fundamentaban en varios supuestos: que la *Glasnost* erosionó el monopolio informativo gubernamental y facilitó la penetración de la propaganda occidental que acabó motivando la caída de la URSS, que la libertad informativa entre 1991 y 2000 hizo a la población vulnerable a la manipulación y a las promesas de prosperidad económica, que internet – utilizado por la juventud como espacio de activismo político y protesta social y considerado por muchos, incluido el presidente Putin como una invención de la CIA para socavar Rusia (MacAskill, 2014) – podía usarse para desestabilizar el país y desmoralizar a la población o que en Chechenia, un adversario militarmente más débil pero informativamente más efectivo y la presencia de periodistas independientes, podían condicionar el curso y desenlace de una operación militar (Giles, 2016; Soldatov; Borogan, 2015; Manojlo, 2014). Estos factores no sólo motivaron la elaboración de la primera *Doctrina de Seguridad de la Información* y la ejecución de una amplia batería de medidas encaminadas a blindar el espacio informativo ruso frente a cualquier amenaza interna e injerencia externa (Vázquez, 2018)[14], sino también el desarrollo de la guerra informativa que, experimentada en Estonia, Georgia, Ucrania o Siria, constituye uno de los pilares de las "guerras de nueva generación" y uno de los fundamentos de los conflictos futuros (Gerasimov, 2019)[15]. Sin embargo, estos interesantes desarrollos estratégicos y militares que se interrelacionan con la adaptación de las medidas activas a la Era de la Información escapan a los objetivos de este trabajo.

Centrando el interés en las medidas activas, desde el final de la Guerra Fría parece que éstas han adaptado progresivamente los instrumentos – especialmente los medios de comunicación, los agentes de influencia o los colaboradores externos[16] – para diseminar desinformaciones, falsificaciones, manipulaciones o datos personales obtenidos de forma ilegal para debilitar adversarios políticos en el mundo físico y digital. Además, también están explotando otros vectores y lenguajes característicos del entorno virtual.

En este sentido, aunque los medios de comunicación continúan siendo fundamentales, sus tácticas han cambiado y su alcance se ha multiplicado. Por un lado, en la actualidad Moscú dispone de medios y plataformas multilingües con fuerte presencia en línea y segmentadas por audiencias tipo (desde la agencia *TASS* o *Russia Beyond* a los populares *Sputnik* o *RT*). Concebidos como una herramienta de poder blando para promover internacionalmente la imagen de Rusia y erosionar el monopolio informativo occidental (Ter, 2018), éstos pueden difundir propaganda blanca (gubernamental) y actuar como altavoz de otras actividades en blogs o redes sociales[17]. Sus narrativas muestran distintos niveles de sofisticación y pueden usar una amplia gama de expertos y comentaristas para otorgar credibilidad a la desinformación (Helmus *et al.*, 2018; Abrams, 2016). Además, hasta fechas recientes muchos periódicos de referencia – como el *Washington Post*, *New York Times*, *Daily Telegraph*, *Le Figaro*, *Repubblica* o *El País* (hasta 2016) – incluían mensualmente el suplemento "Russia Beyond the Headlines". Financiada por el Kremlin, se trataba de un vector de propaganda blanca enfocada a mejorar la imagen de Rusia en el exterior.

Además, Moscú también emplea medios clandestinos para diseminar propaganda gris o negra. Baratos de crear, mantener o replicar y difíciles de atribuir al Kremlin[18], normalmente se los vincula con plataformas de periodismo

---

13 En esta coyuntura, muchos pensadores militares rusos añadieron – interpretando los debates estadounidenses sobre los cambios que se estaban produciendo en el arte bélico motivados por la explotación de las tecnologías de la información en las fuerzas armadas – que estas tecnologías permitirían desestabilizar un país en pocos días o derrotar un oponente militarmente más poderoso sin la necesidad de combatir (Garev, 1998). Estas ideas inspirarían los debates sobre las "guerras de nueva generación" y apoyarían la consolidación de la "guerra informativa".

14 Ello se ha plasmado en el control de las licencias de radiotelevisión y los servicios de telefonía e internet, la vigilancia de la actividad de asociaciones y organizaciones extranjeras en territorio ruso, la promoción del desarrollo de hardware y software nacional o la creación de una muralla digital aparentemente inexpugnable para proteger la moral, cultura y estabilidad social rusa frente a cualquier amenaza interna o externa. Para comprender con más detalle el marco sociopolítico en el que se enmarcan estas acciones, véase Vázquez (2018).

15 En términos muy generales, la guerra informativa (*informatsionnaya voyna*) constituye "…un conflicto entre dos o más estados en el espacio informativo con la finalidad de dañar los sistemas, procesos, recursos o estructuras informativas, erosionar los sistemas políticos, económicos y sociales, llevar a cabo campañas psicológicas masivas contra la población del estado para desestabilizar la sociedad y el gobierno o forzar al estado para que tome decisiones en el interés de sus oponentes." (Ministry of Defence of the Russian Federation, 2011: art. 1). Empleando una amplia variedad de vectores físicos, cibernéticos, electrónicos o psicológicos, la guerra informativa puede servir tanto para alcanzar los objetivos políticos sin la necesidad de emplear la fuerza armada, como para contribuir a la conducción de las operaciones militares (Saifetdinov, 2014; Colom, 2019). Para la evolución de su vertiente propagandístico-informativa, véase Tarín (2018).

16 Además de potenciar medios de comunicación con orientación internacional y amplia presencia en línea, los *proxies* y organizaciones pantalla también se han adaptado con la financiación de partidos políticos populistas, fundaciones, proyectos culturales, ONGs o *think tanks* (Polyakova; Boyer, 2018; Galeotti, 2017, Herpen, 2016). Sin embargo, aunque su estudio escapa de los objetivos de este trabajo, no puede concluirse – algo que también podría argumentarse de otros proyectos procedentes de occidente – que todas estas iniciativas de poder blando sean vectores de medidas activas.

17 Aunque se sostiene que el Kremlin controla la desinformación, cabe preguntarse si el proceso está orquestado para dificultar la atribución, si se permite una cierta discrecionalidad en la creación y difusión de bulos que después serán amplificados por los medios controlados por Moscú o es simple oportunismo (Giles, 2016).

18 Incluso asumiendo que muchos dominios web continúan registrándose en Rusia y pueden compartir detalles de registro e identificador de *google analytics*, es difícil atribuir la responsabilidad al Kremlin. Sin embargo, Washington está intentando establecer una vinculación entre las plataformas registradas por la Agencia de Investigación de Internet (IRA) – propiedad de un oligarca relacionado con Putin y con supuestas vinculaciones con la inteligencia rusa – y el Kremlin (U.S. Department of Justice, 2018; DiResta *et al.*, 2018).

alternativo que difunden bulos, conspiraciones o falsificaciones procedentes de otros blogs y webs (Galeotti, 2017; Jeangène, *et al.*, 2018)[19]. Quizás, también deberían incluirse las plataformas que publican material obtenido por medios ilícitos como *DCleaks* – creada por la inteligencia rusa para apoyar el *hack&leak* del partido demócrata estadounidense (National Intelligence Council [NIC], 2017) – o *Wikileaks*. Aunque no existen vinculaciones concluyentes entre esta plataforma creada por William Assange en 2006 y el Kremlin, si puede afirmarse que ha sido partícipe de contribuir a las medidas activas diseminando documentación obtenida ilegalmente por el Directorado Central de Inteligencia (GRU) ruso para influir en los comicios presidenciales estadounidenses de 2016 (U.S. Department of Justice, 2019: 44-49). Por último, como sucedía en el pasado, también pueden valerse de medios afines en todo el espectro ideológico que divulgan las narrativas rusas voluntariamente, o plataformas legítimas que difunden la desinformación involuntariamente. En este último caso, Rusia parece tenerlo más fácil que en el pasado porque explota la crisis del periodismo tradicional, los nuevos modelos de negocio o la sobreinformación para insertar su propaganda. La difusión de contenidos sin verificar para mantener el ciclo informativo, visibilizar el medio, maximizar el tráfico u obtener *clickbait* (Martens *et al.*, 2018) o por estándares éticos laxos e insuficientes medios a disposición de las plataformas actuales permite al Kremlin emplear numerosos *proxies*[20] para implantar desinformación y falsificaciones en estos medios neutrales (Darczewska; Żochowski, 2018; Helmus *et al.*, 2018).

Los agentes de influencia y los colaboradores también se han adaptado al siglo XXI. Ahora, las personas con proyección pública o autoridad en su disciplina que apoyan clandestinamente a Rusia o simpatizan con ella y difunden sus narrativas son más y tienen mayor visibilidad[21]. Mientras en el pasado las voces amigas oscilaban entre el comunismo y el internacionalismo, ahora se sitúan en todo el espectro político: comunistas, anticapitalistas, extremistas de derechas, antiestadounidenses, antiliberales, populistas, antieuropeos, nacionalistas o defensores de Rusia como último reducto de occidente frente a la posmodernidad, el relativismo o el extremismo islámico (Galeotti, 2017; Abrams, 2016). Todos ellos pueden colaborar en medios y participar en redes sociales diseminando propaganda revestida de aparente objetividad e interactuando con sus seguidores (desdibujando la frontera con los *trolls*) para modelar el debate e influir en la opinión pública (DiResta *et al*., 2018)[22]. Además, artistas, deportistas u otros personajes mediáticos con muchos seguidores en *Facebook*, *Twitter, Instagram* o *Youtube* también pueden ser vectores de desinformación para ciertos sectores de la población menos expuestos a otras fuentes de propaganda (Maese *et al.*, 2017).

Las medidas activas también están utilizando herramientas del mundo virtual para incrementar sus efectos y dificultar la atribución de responsabilidades. En primer lugar, grupos de hackers – como los populares APT-28/*Fancy Bear* o APT-28/*Cozy Bear* – relacionados con el Servicio Federal de Seguridad (FSB), el Servicio de Inteligencia Extranjera (SVR) o el GRU (Fireeye, 2017; Villalón, 2016) se encargan de obtener información sensible. Entre otros objetivos, ésta puede utilizarse para extorsionar a la víctima mediante *kompromat* o difamarla con un *hack&leak*. Empleada también en el entorno físico[23], esta técnica entraña el acceso y filtración de los datos obtenidos – sin manipular como #DCleaks[24] o alterándolos digitalmente como #Macronleaks (Jeangène *et al.*, 2018; NIC, 2017) – en foros, agregadores de noticias, plataformas específicas como *Wikileaks* o *DCleaks* o medios de comunicación generalistas[25] y su posterior amplificación mediante campañas en redes sociales (U.S. Department of Justice, 2019; Select Commitee on Intelligence, 2018; Bradshaw; Howard, 2018).

En segundo lugar, la popular combinación de *trolls* que interactúan con otros usuarios en línea y *bots* automatizados que amplifican el impacto de los primeros. En tres lustros, éstos han pasado de ser jóvenes aficionados que actuaban por convicción en el internet de habla rusa intimidando a periodistas, blogueros y comentaristas críticos con Putin, redistribuyendo información oficialista o alterando el posicionamiento web de páginas contrarias al gobierno, a ser un ejército de *trolls* profesional[26]. Heredera del fallido proyecto de "tropas informativas"[27] que las fuerzas ar-

---

19 Aunque jóvenes macedonios y kosovares creaban sus propios portales y generaban sus propias noticias para obtener ingresos por *clickbait*, también podrían haber sido financiados tanto por la extrema derecha estadounidense como por Moscú (Silverman *et al.*, 2018).

20 Desde *trolls* aparentemente honestos, otros que suplantan la identidad digital de terceros, medios pantalla que replican o reinterpretan noticias de medios locales o blogs para diluir el origen de la desinformación, agentes de influencia, ONGs y *think tanks* que apoyan la narrativa rusa o supuestos *hacktivistas* que filtran información hackeada.

21 Ello no significa que cualquier actor que explique, relativice o contextualice fundamentadamente las actividades rusas pueda desacreditarse acusándole de agente de influencia o colaborador.

22 Giles (2016) añade la posibilidad de alterar progresivamente las percepciones de la ciudadanía sobre Rusia (algo que podría relacionarse con las medidas de poder blando lanzadas por Moscú para intentar mejorar la opinión occidental del país) para crear un "entorno permisivo" para las actividades rusas e incluso influir indirectamente sobre las decisiones políticas mediante el control reflexivo.

23 El KGB intentó infiltrarse en el partido republicano para obtener información que pudiera comprometer a Ronald Reagan. Encaminada a influir en los comicios presidenciales de 1984, esta operación se habría realizado junto con la popularización del eslogan *"Reagan means war"*, la difusión de 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).

24 No obstante, el *hack&leak* del partido demócrata se complementó con actividades de inteligencia, propaganda y desinformación en redes sociales (perfiles y páginas falsas, *microtargeting* sobre perfiles concretos y empleo de *trolls* y *bots* para amplificar el mensaje) y contactos personales con miembros de la campaña de Trump (Select Commitee on Intelligence, 2018; NIC, 2017).

25 Por ejemplo, mediante *guccifer 2.0*, un supuesto *hacktivista* rumano responsable del #DCleaks o *cyberberkut*, *hacktivistas* pro-rusos activos en el conflicto ucraniano. Aunque se hace para dificultar la atribución de responsabilidades, en ambos casos se trata de operativos vinculados con el GRU (Select Commitee on Intelligence, 2018; Fireeye, 2017).

26 Sin embargo, pronto estos *trolls* empezaron a relacionarse con la organización juvenil *nashi* (vinculada con el Kremlin) y profesionalizarse en la denominada "escuela de blogueros del Kremlin", antecesora de este ejército (Giles, 2016).

27 Concebidas para mejorar la política de comunicación militar, éstas incluirían 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 lanzar ciberataques limitados contra los servicios enemigos (Giles, 2016).

madas trataron de implementar tras la guerra de Georgia (2008), esta fuerza maneja varios idiomas, adopta múltiples perfiles y opera globalmente[28].

Asistido por una legión de colaboradores que comparte voluntariamente la propaganda rusa y hostiga a los que cuestionan sus narrativas y por cómplices involuntarios que difunden la desinformación, este ejército continúa participando en foros, blogs o redes sociales generando discusiones, desviando debates y ridiculizando o acosando a los críticos. Sin embargo, ahora también adopta múltiples perfiles – desde reputados usuarios con muchos seguidores que comparten información aparentemente legítima a "*trolls* bikini" con perfiles femeninos para atraer a hombres de mediana edad (Helmus *et al.*, 2018; Giles, 2016) – e interactúa con otros internautas para diseminar contenido falso, proveer relatos alternativos, otorgar credibilidad a la desinformación o suprimir las voces que exponen las inconsistencias de las narrativas falsas (DiResta *et al.*, 2018). Explotando las redes de *bots*, manipulando los rankings de contenido y aprovechándose de la pasividad de las redes sociales para eliminar estas cuentas que siguen patrones distinguibles, esta nueva generación de *trolls* ha conseguido amplificar el alcance de la desinformación para alterar la percepción de la realidad, inducir a la polarización social o crear una falsa impresión de consenso en la red (Jeangène *et al.*, 2018; Helmus *et al.*, 2018).

En último lugar, el referéndum sobre el *Brexit* y los pasados comicios presidenciales estadounidenses sugieren que la propaganda computacional también se ha integrado en las medidas activas (Select Committee on Intelligence, 2018). Basada en el minado de datos para perfilar el usuario, el uso de algoritmos para seleccionar aquellas narrativas que refuercen sus prejuicios y filtrando la difusión de noticias (texto, videos, imágenes o memes), cronología o resultados de búsquedas para manipularlo (Bradshaw; Howard, 2018), la militarización del *microtargeting* amplifica el alcance de la propaganda y refuerza el filtro burbuja. Realizada en connivencia con las empresas tecnológicas, que consiguen nuevos usuarios, más reacciones emocionales y mayores interacciones para obtener perfiles más ricos, y aprovechándose de la ingenuidad humana, partícipe involuntaria de su propio perfilado, del refuerzo de sus prejuicios y de la dispersión de desinformación (en redes sociales, servicios de mensajería o en vivo), la propaganda computacional abre las puertas a campañas masivas de ingeniería social. Sin embargo, no puede afirmarse que estas actividades que contribuyeron a la polarización social y la movilización del electorado provocaran un vuelco en los resultados electorales.

Además, aunque las elecciones presidenciales estadounidenses demostraron –como ya había sucedido en Ucrania dos años antes– el potencial de las medidas activas digitales (U.S. Department of Justice, 2019), para maximizar el impacto, combinar la dimensión física y la lógica y alcanzar aquellas capas de población menos expuestas a internet también se recurrió a medios físicos (operativos como Maria Butina captando agentes de influencia y colaboradores) e informativos (*RT* o *Sputnik* emitiendo por cable). En cualquier caso, las medidas activas están en permanente evolución, explotando las oportunidades que brinda la tecnología y la coyuntura sociopolítica para desinformar, desmoralizar, desestabilizar e influir sobre el adversario.

4. Conclusiones

Aunque apenas han cambiado en su concepción (quizás por la continuidad existente entre la comunidad de inteligencia soviética y rusa), las medidas activas han adaptado sus técnicas al siglo XXI y desarrollado nuevas herramientas para influir en el mundo digital. Han aprovechado el potencial de las nuevas tecnologías para globalizar la propaganda blanca, gris y negra, asimilado el lenguaje de internet para influir sobre el adversario y explotado el poder de las redes sociales – en connivencia con las empresas tecnológicas y la colaboración involuntaria de los usuarios – para posibilitar la manipulación masiva. También han aprovechado las debilidades de las sociedades avanzadas – desde la desafección política o la libertad de expresión a las actitudes posmodernas y relativistas de la ciudadanía – para explotar sus clivajes políticos, socioeconómicos, ideológicos o étnicos apelando a las emociones, denigrando los hechos objetivos, reforzando los prejuicios, encumbrando a conspiradores, planteando realidades alternativas y posibilitando la desinformación. Y todo para influir estratégicamente, desestabilizar socialmente o subvertir políticamente al adversario.

La experiencia acumulada en múltiples escenarios – desde la propaganda en su área de influencia directa, la desinformación en apoyo a las operaciones militares en Ucrania o Siria hasta las intromisiones en procesos políticos – revela que Moscú posee un amplio conjunto de vectores físicos y digitales para apoyar sus actividades de influencia. Su ejército de *trolls*, sus grupos de hackers, sus agencias y servicios de noticias, sus medios encubiertos, su desinformación en línea o su propaganda son los que más atención reciben de los analistas. Sin embargo, forman parte de un complejo ecosistema en constante evolución que combina los nuevos vectores con herramientas tradicionales para alcanzar otras capas de la sociedad menos expuestas a internet. Aunque es posible especular sobre el empleo masivo de *deep fakes*, nuevas tácticas

---

[28] Operativo desde 2013, el IRA – popularmente conocido como la "granja de *trolls* de San Petersburgo" – emplea un millar de trabajadores que participan en medios, blogs, foros o redes sociales. Apoyados por redes de *bots* para amplificar el mensaje, éstos pueden emplearse tanto para fines comerciales como para difundir desinformación en múltiples contextos. Aunque la fiscalía estadounidense califica al IRA como *"...una organización implicada en operaciones para interferir elecciones y procesos políticos"* (U.S. Departament of Justice, 2018: 2) por sus posibles relaciones con la inteligencia rusa y su intromisión en los comicios estadounidenses (empleando sus *trolls* y *bots* pero también perfilando usuarios y comprando publicidad en redes sociales), no debe olvidarse que ésta también apoya la desinformación y el engaño (*maskirovka*) a nivel militar (DiResta *et al.*, 2018.).

de troleo, *bots* que suplantan a seres humanos, mejores perfilados y propagandas computacionales cada vez más refinadas, las medidas activas continuarán sorprendiendo explotando nuestras debilidades, irrumpiendo por donde menos esperamos, utilizando vectores que ignoramos y herramientas que desconocemos. No obstante, conociendo el contexto, historia, objetivos y medios de las medidas activas y comprendiendo el alcance estratégico de la desinformación rusa, quizás será más fácil identificar las campañas, prever sus objetivos y limitar su impacto.

Bibliografía

Abrams, S. (2016). "Beyond propaganda: Soviet active measures in Putin's Russia". En: *Connections*, vol. 15 nº 1, Garmisch-Partenkirchen: PfP Consortium of Defence Academies and Security Studies Institutes, pp. 5-31. http://dx.doi.org/10.11610/Connections.15.1.01

Andrew, C.; Mitrokhin, V. (2000). *The sword and the shield: the Mitrokhin archive and the secret history of the KGB*. Nueva York: Basic Books.

Bezmenov, Y. (1984). *Soviet subversion of the free world press*. Nueva York: American Media, 81 min.

Bittman, L. (1985). *The KGB and Soviet disinformation: an insider's view*. Nueva York: Pergamon.

Boghardt, T. (2009). "Soviet Bloc Intelligence and Its AIDS Disinformation Campaign". En: *Studies in Intelligence*, vol. 53 nº 4, Langley: Central Intelligence Agency, pp. 1-24. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U-%20Boghardt-AIDS-Made%20in%20the%20USA-17Dec.pdf

Bradshaw, S.; Howard, P. (2018). *Challenging truth and trust: a global inventory of organized social media manipulation*. Oxford: Oxford Internet Institute http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf

Bugajski, J. (2004). *Cold Peace: Russia's New Imperialism*. Nueva York: Praeger.

Colom, G. (2019). "Los enfoques estadounidense y ruso de la guerra informativa". En: Torres, M. (coord.). *Desinformación: Poder y manipulación en la era digital*. Granada: Comares, pp. 1-14.

— (2018). "Cuando la realidad supera la ficción: la Operación RYAN (1981-1991)". En: *Ayer*, nº 112, Madrid: Asociación de Historia Contemporánea, pp. 265-293. *http://revistaayer.com/articulo/1313*

Darczewska, J.; Żochowski, P. (2018). *Active Measures: Russia's key export*. Varsovia: Centre for Eastern Studies https://www.osw.waw.pl/sites/default/files/pw_64_ang_active-measures_net_0.pdf

Diresta, R.; Shaffer, K.; Ruppel, B.; Sullivan, D.; Matney, R.; Fox, R.; Albright, J.; Johnson, B. (2018). *The tactics & tropes of the Internet Research Agency*. Austin: New Knowledge. https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper-121718.pdf

Fireeye (2017). *APT28: at the center of the storm. Russia strategically evolves its cyber-operations*. Milpitas: FireEye https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

Galeotti, M. (2017). *Controlling chaos: how Russia manages its political war in Europe*. Londres. European Council on Foreign Relations. https://www.ecfr.eu/page/-/ECFR228_-_CONTROLLING_CHAOS1.pdf

Gareev, M. (1998). *If War Comes Tomorrow? The Contours of Future Armed Conflict*. Londres: Frank Cass.

Gerasimov, V. (2019). "Vektory razvitija voennoj strategii", *Krasnaja zvezda*, 4-3-2019. http://redstar.ru/vektory-razvitiya-voennoj-strategii/

— (2013). "Cennostʹ nauki v predvidenii". En: *Voenno-promyšlennyj kur'er*, vol. 8, nº 476, Moscú: VPK, s.n. https://vpk-news.ru/articles/14632

Giles, K. (2016). *Handbook of Russian information warfare*. Roma: NATO Defence College http://www.ndc.nato.int/download/downloads.php?icode=506

Godson, R. y Shultz, R. (1985). "Soviet active measures: Distinctions and definitions". En: *Defence Analysis*, vol. 1 nº 2, Londres: Taylor & Francis, pp. 101-110. https://doi.org/10.1080/07430178508405191

Helmus, T.; Bodine-Baron, E.; Radin, A.; Magnuson, M.; Mendelsohn, J.; Marcellino, W.; Bega; A.; Winkelman, Z. (2018). *Russian social media influence. Understanding Russian propaganda in Eastern Europe*. Santa Monica: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf

Herpen, M. (2016). *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy*. Lanham: Rowman & Littlefield.

Select Committee on Intelligence (2018). *Report on Russian active measures*, Washington DC: House of Representatives. https://intelligence.house.gov/uploadedfiles/final_russia_investigation_report.pdf

Jeangène, J. B.; Escorcia, A.; Guillaume, M.; Herrera, J. (2018). *Information Manipulation: A Challenge for Our Democracies*. París: CAPS-IRSEM. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736pdf

Jones, S. (2018). *Going on the Offensive*. Washington DC: CSIS. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181002_Russia_Active_Measures_FINAL1.pdf

KGB (1972). *Kontrrazvedyvatel'nyj slovar'*. Moscú: Departamento de publicaciones de la escuela F.E. Dzerzhinsky. http://www.pseudology.org/Abel/KRSlovar2.pdf

Kuleshov, Y.; Zhutdiev, B.; Fedorov, D. (2014). "Informacionno-psihologičeskoe protivoborstvo v sovremennyh usloviâh: teoriâ i praktika". En: *Vestnik Akademii Voennyh Nauk*, vol. 46 nº1, Moscú: Academia de Ciencias Militares, pp. 104-110. http://www.avnrf.ru/attachments/article/639/AVN-1(46)_001-184_print.pdf

Kux, D. (1985). "Soviet active measures and disinformation: overview and assessment". En: *Parameters*, vol. 15 nº 4, Carlisle: Strategic Studies Institute, pp. 19-28. http://www.dtic.mil/dtic/tr/fulltext/u2/a521468.pdf

Macaskill, E. (2014). "Putin calls internet a 'CIA project' renewing fears of web breakup". En: *The Guardian*, 24-4-2014. https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia

Maese, R.; Khurshudyan, I.; Roth, A. "Alex Ovechkin is one of Putin's biggest fans. The question is why?". *The Washington Post*, 25-11-2017. https://www.washingtonpost.com/sports/alex-ovechkin-is-one-of-putins-biggest-fans-the-question-is-why/2017/11/25/*c5f8bb2e-ce36-11e7-9d3a-bcbe2af58c3a_story.html?noredirect=on&utm_term=.d38b28f5e976*

Manojlo, A.B. (2014). *Texnologii nesilovogo razrešenija konfliktov*. Moscú: Hotline-Telecom.

Martens, B.; Aguiar, L.; Gómez, M.; Muller-Langer, F. (2018). *The digital transformation of news media and the rise of disinformation and fake news*. Sevilla: Joint Research Centre Unión Europea. https://ec.europa.eu/jrc/sites/jrcsh/files/jrc111529.pdf

Mitrokhin, V. (ed.) (2002). *KGB Lexicon: The Soviet intelligence officers handbook*. Oxon: Frank Cass.

Ministry of Defence of the Russian Federation (2011). *Conceptual Views regarding the Activities of the Armed Forces of the Russian Federation in Information Space*. Moscú: Ministerio de Defensa. https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

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

Polyakova, A.; Boyer, S. (2018). *The future of political warfare: Russia, the West, and the coming age of global digital competition*. Washington DC: Brookings. https://www.brookings.edu/wp-content/uploads/2018/03/fp_20180316_future_political_warfare.pdf

Rodríguez, R. (2018). "Fundamentos del concepto de desinformación como práctica manipuladora en la comunicación política y las relaciones internacionales". *Historia y comunicación social*, vol. 23 nº 1, Madrid: Universidad Complutense de Madrid, pp. 231-244. https://doi.org/10.5209/HICS.59843

Romerstein, H. (1990). "Soviet Active Measures and Propaganda: "New Thinking" and Influence Activities in the Gorbachev Era". En: Radvanyi, J. (ed.). *Psychological Operations and Political Warfare in Long-term Strategic Planning*. Nueva York: Praeger, pp. 36-68.

Saifetdinov, C. (2014), "Informatsionnoe protivoborstvo v voennoi sfere". En: *Voennaia mysl,* nº 7, pp. 38-41.

Security Information Service (2009). *Annual Report of the Security Information Service for 2008*. Praga: Intelligence Service of the Czech Republic. https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/en/ar2008en.pdf

Shultz, R.; Godson, R. (1984). *Desinformatsia*. Washington DC: Pergamon Brassey's.

Silverman, C.; Feder, L.; Cvetkovska, S.; Belford, A. "Macedonia's pro-Trump fake news industry had American links, and is under investigation for possible Russia ties", *Buzzfeed*, 18-07-2018. https://www.buzzfeednews.com/article/craigsilverman/american-conservatives-fake-news-macedonia-paris-wade-libert

Soldatov, A.; Borogan, I. (2015). *The red web: the struggle between Russia's digital dictators and the new online revolutionaries*. Nueva York: Public Affairs.

Tarín, A. (2018). "Propaganda de guerra: De Chechenia a Siria, pasando por Crimea". En: Tarín, A.; Ter, M.; Vázquez, M. (eds.). *Sistema mediático y propaganda en la Rusia de Putin*. Salamanca: Comunicación Social, pp. 83-108.

Ter, M. (2018). "Propaganda para las audiencias extranjeras". En: Tarín, A.; Ter, M.; Vázquez, M. (eds.). *Sistema mediático y propaganda en la Rusia de Putin*. Salamanca: Comunicación Social, pp. 109-140.

Thomas, T. (2004). "Russia's Reflexive Control Theory and the Military". En: *Journal of Slavic Military Studies*, nº 17, pp. 237–256. http://dx.doi.org.10.1080/13518040490450529237

Thomas, T. (1998). "Russia's information warfare structure: Understanding the roles of the security council, Fapsi, the state technical commission and the military". En: *European Security*, vol. 7 nº 1, Londres: Taylor & Francis, pp. 156-172. https://doi.org/10.1080/09662839808407354

U.S. Department of Justice (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election.* 28 C.F.R. § 600.8(c) https://www.justice.gov/storage/report.pdf

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

U.S. Department of State (1982). *Soviet Active Measures, an update*. nº 101. Washington DC: Government Printing Office. http://insidethecoldwar.org/sites/default/files/documents/Department%20of%20State%20report%20Soviet%20Active%20Measures%20Update%20July%201982.pdf

— (1981). *Soviet Active Measures. Forgery, Disinformation, Political Operations*. Nº 88. Washington DC: Government Printing Office https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf

U.S. Information Agency (1992). *Soviet active measures in the "post-Cold War" era 1988-1991*. Washington DC: Government. Printing Office. https://aktivnyye.com/f/Soviet_Active_Measures_in_the_Post-Cold_War_Era_1988-1991.pdf

U.S. Senate (1985). *Soviet active measures. Hearings before the Subcommittee on European Affairs of the Committee on Foreign Relations.* S-HRG. 99-400. Washington DC: Government Printing Office (5 volúmenes).

Vázquez, M. (2018). "La propaganda de la idea nacional: el 'marco de la guerra'". En: Tarín, A.; Ter, M.; Vázquez, M. (eds.). *Sistema mediático y propaganda en la Rusia de Putin*. Salamanca: Comunicación Social, pp. 53-82.

VILLALÓN, A. (2016). "La Comunidad de Ciberinteligencia rusa", *Security Art Work*, 28-11-2016. https://www.securityartwork.es/2016/11/28/la-cci-rusa-i-introduccion-vienen-los-rusos/

WETTIG, R. (2009). "The last Soviet offensive in the Cold War: emergence and development of the campaign against NATO euromissiles". En: *Cold war history*, vol. 9 nº 1, Londres: Taylor & Francis, pp. 79-110. https://doi.org/10.1080/14682740802638640