



26/2026

6 de marzo de 2026

Eduardo Lobo Almazán

**Guerra por la verdad: anatomía y
defensa frente a la desinformación
rusa**

Guerra por la verdad: anatomía y defensa frente a la desinformación rusa

Resumen:

Este artículo parte de un hecho incómodo: la desinformación rusa se ha convertido en un vector estratégico que explota sesgos cognitivos y fracturas sociales para polarizar, erosionar instituciones y condicionar elecciones en el espacio OTAN-UE. Con ese telón de fondo, el objetivo es doble: desentrañar el ecosistema ruso —producción, distribución y consumo— y contrastar la respuesta europea y aliada para proponer una hoja de ruta operativa. El método combina el análisis del caso del referéndum en los Países Bajos (2016), la tipificación de técnicas psicológicas —repetición, disponibilidad, efecto durmiente, inconsistencias estratégicas— y la revisión de marcos de la UE (Códigos 2018/2022, DSA) y líneas de la OTAN (conciencia situacional, pre-bunking, coordinación). Los resultados muestran un modelo triádico y adaptativo, sostenido por cinco pilares —comunicaciones oficiales, medios estatales, *proxies*, redes sociales y ciberespacio— que fabrica, amplifica y segmenta narrativas con alta eficacia. La conclusión es clara: las respuestas actuales son necesarias pero insuficientes. Para pasar de la reacción fragmentada a la prevención sistemática se requiere anticipación psicológica, fricción algorítmica, verificación priorizada, mando y control conjunto UE-OTAN con células de respuesta rápida y métricas comunes (KPI), integradas en el ciclo preparar–actuar–aprender con apoyo de IA y *big data*.

Palabras clave:

Desinformación, Rusia, Unión Europea (UE), OTAN, guerra híbrida.

***NOTA:** Las ideas contenidas en los **Documentos de Opinión** son responsabilidad de sus autores, sin que reflejen necesariamente el pensamiento del IEEE o del Ministerio de Defensa.

War for the Truth: Anatomy and Defense Against Russian Disinformation

Abstract:

This article starts from an uncomfortable fact: Russian disinformation has become a strategic vector that exploits cognitive biases and social fractures to polarize, erode institutions, and shape elections across the NATO–EU space. Against that backdrop, the aim is twofold: to unpack Russia’s ecosystem—production, distribution, and consumption—and to contrast European and allied responses to propose an operational roadmap. The method combines case analysis (Netherlands 2016), typifies psychological techniques—repetition, availability, sleeper effect, strategic inconsistencies—and reviews EU frameworks (2018/2022 Codes, DSA) and NATO lines of effort (situational awareness, pre-bunking, coordination). Findings indicate a triadic, adaptive model, anchored in five pillars—official communications, state media, proxies, social networks, and cyberspace—that effectively manufactures, amplifies, and segments narratives. The conclusion is clear: current responses are necessary but insufficient. Moving from fragmented reaction to systematic prevention requires psychological anticipation, algorithmic friction, prioritized verification, NATO–EU command and control with rapid-response cells, and shared metrics (KPIs), all embedded in a Prepare–Act–Learn cycle supported by AI and big data.

Keywords:

Disinformation, Russia, European Union (EU), NATO, Hybrid Warfare.

Cómo citar este documento:

LOBO ALMAZÁN, Eduardo. *Guerra por la verdad: anatomía y defensa frente a la desinformación rusa*. Documento de Opinión IEEE 26/2026. [enlace web IEEE](#) y/o [enlace bic³](#) (consultado día/mes/año)

Introducción

La guerra por la verdad ya no se decide en los despachos, sino en la mente del ciudadano. El modelo ruso *Firehose of Falsehood* convierte la repetición, la disponibilidad y el sesgo de confirmación en munición de precisión: una avalancha multicanal que explota la emoción, la distracción y las burbujas informativas para colonizar la agenda. Este artículo desnuda esa ingeniería psicológica —del efecto de verdad ilusoria al durmiente— y muestra por qué, incluso cuando los mensajes contradictorios aparecen, ganan tracción cuando la fuente goza de autoridad percibida.

Rusia no emite mensajes aislados: opera un ecosistema industrial —«producción, distribución y consumo»— que fabrica relatos, los amplifica mediante *proxies* y *bots* y los inserta en audiencias segmentadas para maximizar la polarización y la erosión institucional. Se radiografía la cadena de valor desinformativa —de la difamación y la contradicción estratégica a la amplificación y su consumo dirigido— para entender una influencia rápida, flexible y de difícil atribución.

El siglo XXI ha convertido la desinformación en vector estratégico: Rusia explota las fisuras de las democracias de la OTAN y la UE para polarizar, deslegitimar instituciones y condicionar elecciones democráticas. El caso de los Países Bajos evidencia cómo una narrativa manufacturada —euroescepticismo, vídeos fabricados, cuentas «zombi», encuadre emocional— penetra en el debate público y desplaza la realidad. Estos ejemplos ofrecen una lectura operativa de esas campañas para extraer palancas de resiliencia y blindaje electoral.

Europa ha alzado una arquitectura dual frente a la desinformación: una UE reguladora que combina autorregulación (Códigos 2018/2022) y *hard law* (DSA), y una OTAN operativa que articula la comprensión del entorno y la implicación pública con la coordinación multinivel. Aquí se contrastan el modelo normativo y el operativo, y se explica cómo se complementan para proteger el ecosistema informativo sin erosionar las libertades.

Por último, el artículo transita del diagnóstico a la prescripción con un enfoque de toda la alianza y toda la sociedad, anclado en el ciclo «preparar–actuar–aprender»: educación y alfabetización mediática, comunicación estratégica interoperable, innovación tecnológica y coherencia normativa UE–OTAN para pasar de la reacción tardía a la prevención sistemática.

La desinformación

El primer paso para diseñar una estrategia eficaz contra la desinformación es conocer la amenaza. El modelo propagandístico ruso, denominado *Firehose of Falsehood* o «manguera de falsedad», resulta eficaz porque manipula sesgos y heurísticos psicológicos que dificultan distinguir verdad de la falsedad¹. La psicología explica por qué este enfoque logra moldear la opinión pública e influir en el comportamiento.

Rusia difunde una «avalancha de contenidos en múltiples plataformas», incrementando la probabilidad de que sus narrativas sean interiorizadas. Basado en la exposición selectiva, este método explota la repetición y el heurístico de disponibilidad: cuanto más se repite un mensaje, más creíble parece. La familiaridad reduce el pensamiento crítico, y el sesgo de confirmación consolida el impacto cuando el mensaje coincide con creencias previas.

Este modelo «difunde información de forma rápida, continua y repetitiva». La repetición continua provoca el efecto de verdad ilusoria, por el cual las afirmaciones repetidas se perciben como ciertas, especialmente entre audiencias pasivas. Los sesgos cognitivos, las primeras impresiones y las burbujas informativas refuerzan creencias previas y aíslan de visiones alternativas. Reiterar falsedades disminuye su percepción de inmoralidad y facilita su propagación.

La propaganda rusa «ignora la verdad objetiva y explota diversos sesgos psicológicos». El efecto durmiente explica cómo las personas recuerdan el mensaje, pero olvidan su fuente, lo que prolonga su impacto². Unido al sesgo de confirmación, favorece la aceptación de narrativas que encajan con creencias previas, reduciendo la disonancia cognitiva³. Al recurrir a emociones como el miedo o la ira, refuerza ideologías y percepciones existentes⁴. En contextos de crisis e incertidumbre, cuando los mensajes oficiales son confusos, la desinformación se propaga con mayor eficacia, como demostró

¹ PAUL, Christopher y MATTHEWS, Miriam. *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. Santa Monica (CA), RAND Corporation, 2016, p. 2. Disponible en: <https://doi.org/10.7249/PE198>.

Nota: Todos los hipervínculos de este artículo se encuentran activos con fecha de 14 de enero de 2026.

² PAUL y MATTHEWS. *The Russian "Firehose of Falsehood"...*, 2016, p. 6.

³ NICKERSON, Raymond. «Confirmation Bias: A Ubiquitous Phenomenon in Many Guises», *Review of General Psychology*, vol. 2. Junio de 1998, p. 211. Disponible en: <https://doi.org/10.1037/1089-2680.2.2.175>; FESTINGER, Leon. *A Theory of Cognitive Dissonance*. Stanford (CA), Stanford University Press, 1957, p. 31.

⁴ WESTFALL, Jacob et al. «Perceiving Political Polarization in the United States: Party Identity Strength and Attitude Extremity Exacerbate the Perceived Partisan Divide», *Perspectives on Psychological Science*, vol. 10, n.º 2. Marzo de 2015, pp. 145 y 155. Disponible en: <https://doi.org/10.1177/1745691615569849>.

la pandemia del COVID-19⁵. Esta estrategia maximiza su efecto al aprovechar la vulnerabilidad emocional y cognitiva del público.

Por último, la propaganda rusa «es inconsistente». La inconsistencia también refuerza su impacto. Aunque contradiga la repetición, puede estimular el interés público y la curiosidad, incrementando la credibilidad percibida⁶. Esto se observó en los mensajes cambiantes sobre el vuelo MH17 de Malaysia Airlines⁷. De modo similar, en el caso de la anexión de Crimea (2014), las narrativas inconsistentes del presidente Putin ilustran cómo la inconsistencia no necesariamente daña la influencia cuando señales periféricas —como la autoridad percibida de la fuente— refuerzan la credibilidad⁸. Esta flexibilidad permite adaptar narrativas a los objetivos estratégicos del Kremlin, manteniendo credibilidad a través de medios como *RT* y *Sputnik*⁹.

En síntesis, el modelo ruso de desinformación se sustenta en la explotación de heurísticos psicológicos que monopolizan la atención, moldean creencias y mantienen su influencia incluso cuando los mensajes son falsos o contradictorios. Comprender estos mecanismos es esencial para diseñar estrategias eficaces de detección y defensa.

Un enfoque regional. El caso de Rusia

La desinformación rusa opera como un ecosistema compuesto por tres partes: producción, distribución y consumo¹⁰. Manipula la información, la difunde mediante técnicas de diseminación adaptadas y la dirige contra audiencias diversas para influir en sus percepciones.

⁵ DEPARTAMENTO DE SEGURIDAD NACIONAL, Gobierno de España. *Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional: Trabajos 2023*. Madrid (España), Consejo de Seguridad Nacional, 2023, p. 18. Disponible en: <https://www.dsn.gob.es/es/documento/foro-contra-campa%C3%B1as-desinformaci%C3%B3n-%C3%A1mbito-seguridad-nacional-trabajos-2023>.

⁶ REICH, Taly y TORMALA, Zakary, L. «When Contradictions Foster Persuasion: An Attributional Perspective», *Journal of Experimental Social Psychology*, vol. 49, n.º 3. Mayo de 2013, pp. 426 y 438. Disponible en: <https://doi.org/10.1016/j.jesp.2013.01.004>.

⁷ PAUL y MATTHEWS. *The Russian "Firehose of Falsehood"...*, 2016, p. 8.

⁸ RUCKER, Derek D., PETTY, Richard E. y BRIÑOL, Pablo. «What's in a Frame Anyway?: A Meta-Cognitive Analysis of the Impact of One versus Two Sided Message Framing on Attitude Certainty», *Journal of Consumer Psychology*, vol. 18, n.º 2. Abril de 2008, pp. 147–148. Disponible en: <https://doi.org/10.1016/j.jcps.2008.01.008>.

⁹ PAUL y MATTHEWS. *The Russian "Firehose of Falsehood"...*, 2016, p. 9.

¹⁰ MATTHEWS, Miriam et al. *Understanding and Defending Against Russia's Malign and Subversive Information Efforts in Europe*. Santa Monica (CA), RAND Corporation, 2021, p. 66. Disponible en: https://www.rand.org/pubs/research_reports/RR3160.html.

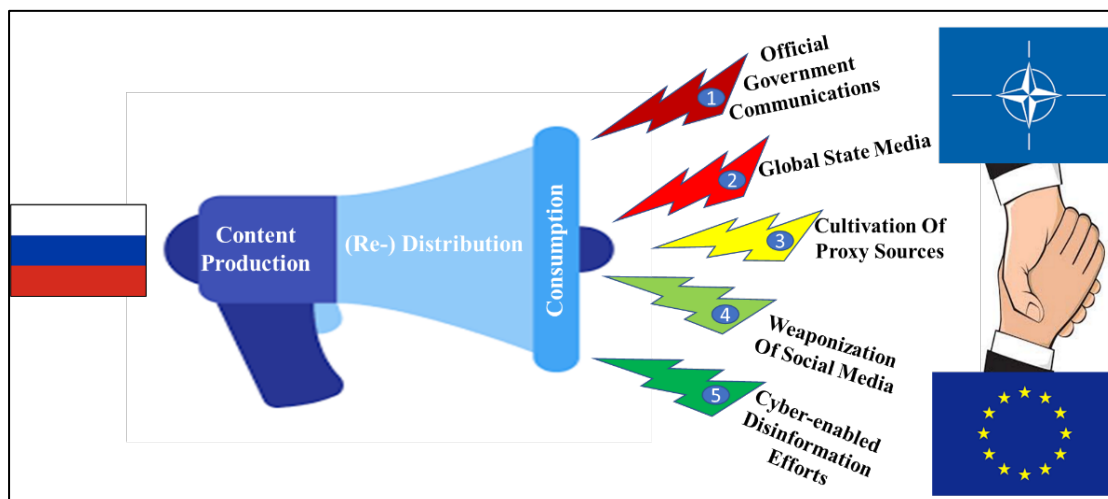


Imagen 1. Modelo patológico de los esfuerzos desinformativos malintencionados de Rusia. Creada por el autor.

Respecto a la fase de «producción», las campañas de desinformación rusas crean y manipulan la información para alcanzar fines estratégicos, difamando a gobiernos, actores no gubernamentales y políticas, mientras fomentan la discordia y promueven actores afines a Moscú¹¹. En las elecciones francesas de 2017, medios rusos acusaron a Emmanuel Macron de ser un «agente estadounidense», empleando tópicos antisemitas para erosionar su credibilidad y polarizar al electorado, lo cual incitó a la acción política de teóricos de la conspiración de derecha y explotó las divisiones sociales¹².

A la vez, Rusia amplifica narrativas positivas sobre su identidad, cultura, instituciones y logros, apelando a vínculos históricos con sus audiencias y utilizando grandes eventos internacionales como instrumentos de proyección de poder¹³. Por ejemplo, Rusia glorifica sus eventos internacionales para proyectar poder y desviar las críticas¹⁴.

Para confundir, genera y difunde versiones contradictorias, como en el caso del envenenamiento de Sergei Skripal, creando incertidumbre y desconfianza¹⁵. Mediante

¹¹ MATTHEWS, et al. *Understanding and Defending...*, 2021, p. 20.

¹² SPUTNIK INTERNATIONAL. «Ex-French Economy Minister Macron Could Be “US Agent” Lobbying Banks’ Interests». 2 de abril de 2017. Disponible en: <https://sputnikglobe.com/20170204/macron-us-agent-dhuicg-1050340451.html>; LOCKWOOD, Erin. «The Antisemitic Backlash to Financial Power: Conspiracy Theory as a Response to Financial Complexity and Crisis», *New Political Economy*, vol. 26, n.º 2. 2021, p. 261. Disponible en: <https://doi.org/10.1080/13563467.2020.1841141>.

¹³ MATTHEWS, et al. *Understanding and Defending...*, 2021, p. 20.

¹⁴ SPUTNIK INTERNATIONAL «Success of the World Cup Is “a Nail in Coffin of Mainstream Medi» – *Journalist*. 18 de julio de 2018. Disponible en: <https://sputnikglobe.com/20180718/russia-world-cup-mainstream-media-1066453434.html>.

¹⁵ JOSHI, Shashank. «Skripal: The Weight of Evidence», *The Interpreter*. 5 de abril de 2018. Disponible en: <https://www.lowyinstitute.org/the-interpreter/skripal-weight-evidence>;

MATTHEWS, Miriam et al. *Understanding and Defending...*, 2021, p. 20.

medios estatales y *bots*, difundieron mensajes que desacreditaron a las autoridades europeas con la intención de debilitar la cohesión euroatlántica¹⁶.

La producción de contenidos combina la fabricación, tergiversación y selección parcial de hechos, explotando la emoción y la confusión como armas de influencia global¹⁷.

Con respecto a la «distribución», Rusia distribuye su desinformación mediante una red diversa de actores y canales adaptados a cada contexto¹⁸. Así, medios controlados por el Estado, como *RT* y *Sputnik*, difunden abiertamente contenidos manipulados para moldear percepciones globales favorables al Kremlin¹⁹.

Otros actores, como la Internet Research Agency (IRA) o WikiLeaks, operan como intermediarios con vínculos opacos²⁰. Por ejemplo, en las elecciones estadounidenses de 2016, emplearon acertadamente perfiles falsos para difundir mensajes divisivos y debilitar a Hillary Clinton, alineándose con los intereses estratégicos de Rusia²¹.

Asimismo, figuras y medios no afiliados, incluidos influenciadores de ideologías extremas en Europa y EE. UU., pueden amplificar involuntariamente las narrativas rusas, a veces con financiación encubierta. Influenciadores de derecha como Benny Johnson, Tim Pool y Dave Rubin, actores no estatales que, sin saberlo, participaron en operaciones de influencia rusa cuando medios estatales rusos financiaron de forma encubierta sus vídeos en inglés que promovían puntos de vista prorrusos²².

¹⁶ JEANGÈNE VILMER, J. B. *et al.* *Information Manipulation: A Challenge for Our Democracies*. París (Francia), The Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, 2018, p. 94. Disponible en:

https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

¹⁷ MATTHEWS, *et al.* *Understanding and Defending...*, 2021, p. 26.

¹⁸ MATTHEWS, *et al.* *Understanding and Defending...*, 2021, p. 31.

¹⁹ RAMSAY, Gordon, y ROBERTSHAW, Samuel. *Weaponising News: RT, Sputnik, and Targeted Disinformation*. Londres (Reino Unido), Policy Institute, King's College London, 2019, p. 107. Disponible en:

<https://www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf>.

²⁰ SHERMAN, Justin. *Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior*. Washington, D.C., Atlantic Council, 2022, pp. 10–11. Disponible en: <https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Untangling-the-Russian-Web-Spies-Proxies-and-Spectrums-of-Russian-Cyber-Behavior-1.pdf>.

²¹ JANKOWICZ, Nina. *How to Lose the Information War: Russia, Fake News, and the Future of Conflict*. Londres (Reino Unido), I. B. Tauris, 2020, p. 9. Disponible en: eBook Collection (EBSCOhost): <https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=nlebk&AN=2471429&authtype=athens&site=ehost-live&scope=site&custid=s2983631>.

²² LYNKAAS, Sean y PASSATINO, Jonathan. «Right-Wing Influencers Say They Were Dupes in an Alleged Russian Influence Operation. They Are Keeping Their Millions for Now», *CNN*. 13 de septiembre de 2024. Disponible en: <https://www.cnn.com/2024/09/13/media/right-wing-media-influencers-tenet-russian-money/index.html>; SUDERMAN, Alan y SWENSON, Alison. «Right-Wing Influencers Were Duped to Work for Covert Russian Operation, US Says», *Associated Press*. Septiembre de 2024. Disponible en: <https://apnews.com/article/russian-interference-presidential-election-influencers-trump-999435273dd39edf7468c6aa34fad5dd>.

Rusia utiliza medios tradicionales, plataformas digitales y redes sociales como principales canales para alcanzar a sus audiencias objetivo²³. Ejemplos incluyen los mensajes engañosos del Ministerio de Asuntos Exteriores ruso tras el caso Skripal en *Twitter* (ahora X), o la difusión masiva de contenidos por RT y YouTube²⁴. Asimismo, foros organizados por *proxies* y comunicados oficiales refuerzan esta estrategia²⁵.

En conjunto, la multiplicidad de actores y plataformas permite a Rusia diseminar su desinformación de forma eficaz, ocultar su origen y generar la apariencia de movimientos espontáneos alineados con sus intereses estratégicos.

Por último, el «consumo» de la desinformación rusa constituye la fase final del ecosistema. Las audiencias objetivo absorben contenidos diseñados para manipular la opinión pública y reforzar la polarización. Rusia orienta sus mensajes hacia grupos demográficos específicos mediante narrativas culturales, históricas y políticas que consolidan sesgos y desconfianza institucional.

Su alcance incluye al público general, élites e influenciadores²⁶. En Europa, explota tanto a la extrema derecha como a la izquierda, con mensajes antioccidentales y antisistema, generando cámaras de eco que amplifican la discordia y minan la confianza en la OTAN y la UE²⁷. Las elecciones estadounidenses de 2020 ilustran esta dinámica: la interferencia rusa buscó debilitar a Joe Biden mediante granjas de *trolls* y redes sociales controladas por la IRA, repitiendo tácticas ya empleadas en 2016 para dividir y reducir la participación electoral²⁸.

²³ MATTHEWS, et al. *Understanding and Defending...*, 2021, pp. 36–37.

²⁴ MINISTRY OF FOREIGN AFFAIRS OF THE RUSSIAN FEDERATION (@mfa_russia). «In connection with the accusations of poisoning S. #Skripal and his daughter in #Salisbury, we suggest you to read the article published in 2004 by the #UK 'Guardian' on the activities of the Defence Science and Technology Laboratory in Porton Down». <https://theguardian.com/science/2004/may/06/science.research> <https://t.co/ht2hZ7193y>. Twitter/X, 27 de marzo de 2018. Disponible en: https://x.com/mfa_russia/status/978502879655944192; MATTHEWS, et al. *Understanding and Defending...*, 2021, p. 37.

²⁵ MATTHEWS, et al. *Understanding and Defending...*, 2021, pp. 32–33.

²⁶ MATTHEWS, et al. *Understanding and Defending...*, 2021, p. 38.

²⁷ ROBINSON, Linda et al. *Modern Political Warfare: Current Practices and Possible Responses*. Santa Monica (CA), RAND Corporation, 2018, p. 66. Disponible en: https://www.rand.org/pubs/research_reports/RR1772.html.

²⁸ BURRETT, Tina. «Feeling the Bern? Russian Media Reporting on the U.S. Democratic Party's Presidential Primaries», *Russian Analytical Digest*, n.º 253. Junio de 2020, p. 14; BURRETT. *Feeling the Bern?*, 2020, p. 14; HARRIS, Shane et al. «Bernie Sanders Briefed by US Officials that Russia is Trying to Help His Presidential Campaign», *The Washington Post*. Febrero de 2020. Disponible en: https://www.washingtonpost.com/national-security/bernie-sanders-briefed-by-us-officials-that-russia-is-trying-to-help-his-presidential-campaign/2020/02/21/5ad396a6-54bd-11ea-929a-64efa7482a77_story.html.

Rusia también apela a vínculos culturales, religiosos e históricos. Narrativas como las anti-LGTBQ+ resuenan en Europa del Este, donde se proyecta a Moscú como defensora de los valores tradicionales frente a una «Gayropa» decadente²⁹.

El uso de *bots*, *astroturfing*, cuentas automatizadas y manipulación de los algoritmos en redes sociales amplifica la difusión³⁰. Con esto consigue generar la apariencia humana de los mensajes, como se evidenció en EE. UU. (2016 y 2020). Los *bots* inundaron las redes con contenido divisivo, ampliando su alcance y logrando involucrar a audiencias inadvertidas, cuyas voces reforzaron la legitimidad de los mensajes³¹.

Los métodos empleados por Rusia se adaptan al entorno mediático: medios tradicionales en el Este, redes sociales en el Oeste³². Su eficacia varía; en regiones prorrusas como Hungría, donde los medios locales replican abiertamente las narrativas, la influencia de la desinformación rusa es considerablemente mayor³³; en aquellas zonas menos receptivas se requieren métodos encubiertos que crean esa sensación de apoyo³⁴. Sin embargo, en los países bálticos o Finlandia, el público las rechaza, reflejado en el descenso de apoyo a símbolos soviéticos, como evidencia el descenso de participación en las celebraciones del 9 de mayo, fecha de la victoria soviética sobre Alemania³⁵.

Claramente, la maquinaria de desinformación rusa opera mediante un ecosistema sofisticado de producción, distribución y consumo, sustentado en cinco pilares clave: comunicaciones oficiales, medios estatales globales, fuentes *proxy*, redes sociales y ciberespacio³⁶. Su estructura le permite proyectar una narrativa flexible, descentralizada

²⁹ MATTHEWS, et al. *Understanding and Defending...*, 2021, pp. 38–39; DI MARCOBERNARDINO, Andrea. «Anti-LGBTQ+ Propaganda: How Russia Persecutes SOGI Minorities as Part of Its Anti-Western Rhetoric», *The Security Distillery*, 29 de junio de 2024. Disponible en: <https://thesecuritydistillery.org/all-articles/anti-lgbtq-propaganda-how-russia-persecutes-sogi-minorities-as-part-of-its-anti-western-rhetoric>; STRAND, Cecilia et al. *Disinformation Campaigns About LGBTI+ People in the EU and Foreign Influence*. Briefing PE653.644. Bruselas (Bélgica), European Parliament, 2021, p. 7. Disponible en:

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/653644/EXPO_BRI\(2021\)653644_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/653644/EXPO_BRI(2021)653644_EN.pdf).

³⁰ LAZER, David M. J. et al. «The Science of Fake News», *Science*, vol. 359, n.º 6380. Marzo de 2018, p. 1095. Disponible en: <https://doi.org/10.1126/science.aao2998>.

³¹ SHAO, Chengcheng, et al. «The Spread of Low-Credibility Content by Social Bots», *Nature Communications*, vol. 9, n.º 1. Noviembre de 2018, pp. 1-2. Disponible en: <https://doi.org/10.1038/s41467-018-06930-7>.

³² MATTHEWS, et al. *Understanding and Defending...*, 2021, p. 39.

³³ MATTHEWS, et al. *Understanding and Defending...*, 2021, p. 40.

³⁴ KREKÓ, Péter, et al. *The Weaponization of Culture: Kremlin's Traditional Agenda and the Export of Values to Central Europe*. Budapest (Hungría), Political Capital, 2016, p. 7. Disponible en: https://politicalcapital.hu/wp-content/uploads/PC_reactionary_values_CEE_20160727.pdf.

³⁵ MATTHEWS, et al. *Understanding and Defending...*, 2021, p. 40; JEANGÈNE VILMER, et al. *Information Manipulation...*, 2018, p. 66.

³⁶ GLOBAL ENGAGEMENT CENTER. *GEC Special Report: Russia's Pillars of Disinformation and Propaganda Ecosystem*. Washington, D.C., Department of State, agosto de 2020, p. 8. Disponible en: https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

y difícil de atribuir. Los medios estatales refuerzan mutuamente estas narrativas, respondiendo rápidamente a objetivos políticos y manteniendo un enfoque constante en desacreditar a los adversarios percibidos. Y, aunque la UE haya sancionado a medios como RT y Sputnik, Rusia se adapta mediante nuevos dominios y plataformas, explotando los tiempos de respuesta más lentos de las democracias occidentales³⁷. Pese a resultados dispares, la desinformación rusa sigue siendo un instrumento estratégico de *Soft Power* o *Smart Power*, que erosiona la cohesión social y desafía la resiliencia democrática global.

Un enfoque práctico. El siglo XXI

Desde el fin de la Guerra Fría y el ascenso de Putin, la desinformación rusa ha tenido como blanco a los países de la OTAN y la UE. Su propósito ha sido explotar divisiones sociales, debilitar la cohesión, polarizar la política y erosionar alianzas para alcanzar objetivos geopolíticos. Comprender estas campañas es esencial para diseñar una estrategia eficaz. El caso del referéndum celebrado en los Países Bajos ofrece lecciones clave para fortalecer la resiliencia, promover la alfabetización digital, proteger los procesos electorales y equilibrar las contramedidas con los valores democráticos.

El referéndum holandés de 2016 sobre el Acuerdo de Asociación UE-Ucrania ejemplifica cómo Rusia explotó el euroescepticismo para influir en la opinión pública. A través de medios como RT y Sputnik, amplificó narrativas que presentaban a Ucrania como corrupta y dependiente, difundiendo falsedades como la supuesta crucifixión de un niño o vídeos manipulados con soldados del batallón Azov quemando una bandera holandesa³⁸. Aunque Bellingcat desmintió estos contenidos y los vinculó a la IRA, la campaña reforzó los esfuerzos rusos al mostrar a Ucrania como un riesgo para la estabilidad europea³⁹.

³⁷ COUNCIL OF THE EUROPEAN UNION. *Council Decision (CFSP) 2022/351 of 1 March 2022 Amending Decision 2014/512/CFSP Concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine*. Official Journal of the European Union, serie L, n.º 65, febrero de 2022, pp. 6–7. Disponible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D0351&qid=1727289198407>; COUNCIL OF THE EUROPEAN UNION. *Council Decision (CFSP) 2023/1566 of 28 July 2023 Amending Decision 2014/145/CFSP Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine*. Official Journal of the European Union, serie L, n.º 190 I, julio de 2023, pp. 21–27. Disponible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023D1566>.

³⁸ HIGGINS, Andrew. «Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote», *The New York Times*, sección World. Nueva York (NY), 16 de febrero de 2017. Disponible en: <https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html>.

³⁹ BELLINGCAT INVESTIGATION TEAM. «Behind the Dutch Terror Threat Video: The St. Petersburg “Troll Factory” Connection», *Bellingcat*. 3 de abril de 2016. Disponible en: <https://www.bellingcat.com/news/uk-and-europe/2016/04/03/azov-video>; DELOY, Corinne y JOANNIN, Pascale. «The Dutch Reject the Association Treaty



Imagen 2. Imagen fabricada de miembros del Batallón Azov quemando la bandera holandesa⁴⁰.

Rusia también aprovechó movimientos euroescépticos locales. El blog *GeenStijl* replicó la retórica anti-UE y las narrativas de Putin, describiendo el acuerdo como una amenaza a la soberanía rusa y a la identidad europea como producto del Euromaidán, además de tildar al gobierno ucraniano de neonazi⁴¹. Figuras políticas como Harry van Bommel (parlamentario de izquierdas) y Thierry Baudet (líder del partido Foro por la Democracia) amplificaron estos mensajes, otorgándoles legitimidad y contribuyendo al rechazo del acuerdo⁴².

El caso holandés demuestra cómo Rusia utiliza sesgos psicológicos como el efecto de verdad ilusoria y la exposición selectiva, entre otros, para reforzar prejuicios anti-UE y antiucranianos. Mediante narrativas contradictorias y mensajes adaptados, el Kremlin alineó sus esfuerzos con el Modelo Estratégico de Desinformación rusa descrito, alimentando la confusión y la desconfianza hacia la UE.

Las lecciones del referéndum evidencian la necesidad de adoptar medidas integrales contra la desinformación: análisis de vulnerabilidad, planes de contingencia, marcos legales y educación ciudadana. Fortalecer la resiliencia requiere también formar a los

between the EU and Ukraine», *Policy Paper* 388, European Issues. París (Francia), Foundation Robert Schuman, 2016, p. 2. Disponible en: <https://server.www.robert-schuman.eu/storage/en/doc/questions-d-europe/qe-388-en.pdf>.

⁴⁰ BELLINGCAT INVESTIGATION TEAM. *Behind the Dutch Terror...*, 2016.

⁴¹ VASSEUR, Tom. «The Dutch-Ukraine Referendum: Between Apathy and Antipathy», *Green European Journal*. 30 de marzo de 2016. Disponible en: <https://www.greeneuropeanjournal.eu/the-dutch-ukraine-referendum-between-apathy-and-antipathy>.

⁴² HIGGINS. *Fake News, Fake Ukrainians...*, 2017.

partidos, proteger a los medios, cooperar con las plataformas digitales y promover la colaboración internacional en buenas prácticas⁴³.

Un enfoque estratégico. La Unión Europea y la OTAN

La UE afronta la desinformación mediante un enfoque mixto que combina autorregulación voluntaria y legislación obligatoria, buscando proteger el entorno informativo europeo sin vulnerar derechos fundamentales como la libertad de expresión.

Su marco se basa en el *Código de buenas prácticas sobre la desinformación* (2018) y su *versión reforzada* (2022), junto con la *Ley de Servicios Digitales* (DSA, 2022)⁴⁴. Los códigos voluntarios recomiendan que, plataformas como «Meta, Google, X y TikTok», se sumen a la desmonetización de la desinformación, la transparencia en la publicidad política y el apoyo a verificadores e investigadores⁴⁵. El código reforzado amplió estos compromisos a 44 medidas, creando un centro de transparencia y priorizando la alfabetización mediática, la eliminación de cuentas falsas y la promoción de información fiable.

La DSA, complementariamente, impone obligaciones vinculantes a las plataformas digitales, especialmente a las de gran tamaño, sobre moderación de contenidos, transparencia publicitaria y gestión de riesgos mediante auditorías independientes. Su propósito es garantizar un espacio digital seguro, predecible y respetuoso con la Carta de Derechos Fundamentales de la UE.

Además, la UE ha actuado frente a amenazas concretas como la desinformación rusa. Prohibió la emisión de RT y Sputnik tras la invasión de Ucrania y, en 2022, impulsó la

⁴³ BRATTBERG, Erik, y MAURER, Timothy. *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*. Washington, D.C., Carnegie Endowment for International Peace, 2018, pp. 1–2 y 29–32. Disponible en: <https://carnegieendowment.org/research/2018/05/russian-election-interference-europes-counter-to-fake-news-and-cyber-attacks?lang=en>.

⁴⁴ EUROPEAN COMMISSION. *2018 Code of Practice on Disinformation*. Bruselas (Bélgica), European Commission, 2018. Disponible en: <https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation>; EUROPEAN COMMISSION. *2022 Strengthened Code of Practice on Disinformation*. Bruselas (Bélgica), European Commission, 2022. Disponible en: <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>; THE COUNCIL OF THE EUROPEAN UNION. *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)*. Official Journal of the European Union, serie L 277, octubre de 2022, pp. 1–102.

⁴⁵ DEPARTAMENTO DE SEGURIDAD NACIONAL. *Foro contra las Campañas de Desinformación...*, 2023, p. 256.

creación de la Red Europea de Estándares de Verificación de Hechos (EFCSN), que agrupa a 45 medios de 30 países bajo un código ético común⁴⁶.

Por último, el proyecto de Ley de Inteligencia Artificial (2021) refuerza este compromiso al exigir que los contenidos generados por IA sean claramente identificables, adaptando la regulación a los nuevos desafíos tecnológicos⁴⁷.

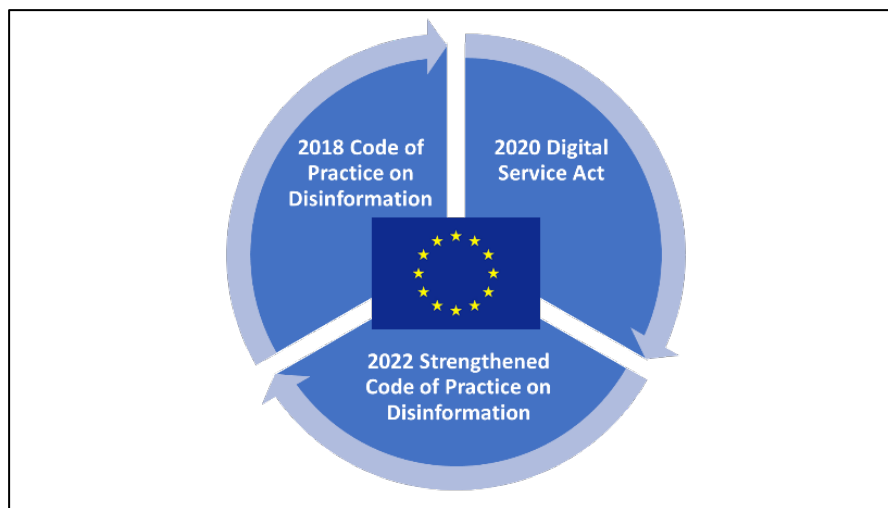


Imagen 3. La estrategia de la Unión Europea. Creada por el autor

En síntesis, la estrategia de la UE contra la desinformación evoluciona de forma cíclica: desde la autorregulación de 2018 hasta la regulación plena de la DSA, perfeccionando continuamente sus herramientas para fortalecer la transparencia, la confianza y la integridad del ecosistema informativo europeo. No obstante, como la desinformación continúa haciendo daño, esta estrategia es insuficiente.

Aunque no existe un documento único, «la estrategia de la OTAN» frente a la desinformación se basa en un modelo de doble vía centrado en la comprensión y la implicación, reforzado por diversos elementos estratégicos que aumentan su capacidad para afrontar la guerra informativa en el entorno actual de seguridad⁴⁸.

⁴⁶ EUROPEAN FACT-CHECKING STANDARDS NETWORK (EFCSN). «Frequently Asked Questions. What Is the EFCSN?», *European Fact-Checking Standards Network (EFCSN)*, consultado el 27 de septiembre de 2024. Disponible en: <https://efcsn.com>.

⁴⁷ DEPARTAMENTO DE SEGURIDAD NACIONAL, «Foro contra las Campañas de Desinformación...», 2023, p. 25.

⁴⁸ NATO. *NATO's Approach to Countering Disinformation*. NATO, noviembre de 2023. Disponible en: https://www.nato.int/cps/en/natohq/topics_219728.htm.

La comprensión del entorno informativo es el «primer pilar»⁴⁹. Mediante su capacidad de evaluación, la OTAN analiza de forma continua las fuentes de desinformación, las narrativas hostiles y los comportamientos emergentes. El *Concepto Estratégico de 2022*, aprobado en la Cumbre de Madrid, identifica a Rusia como actor clave y subraya la necesidad de contrarrestar tácticas híbridas⁵⁰. Ejemplos concretos de respuesta institucional incluyen la Rapid Response Unit británica, que detecta campañas rusas; las Fuerzas Armadas de Lituania, que monitorizan la propaganda; y la Oficina del Director de Inteligencia Nacional de EE. UU., que incluye a Rusia entre las principales amenazas.

El «segundo pilar» es la implicación pública, basada en la comunicación transparente y anticipatoria (*pre-bunking*)⁵¹. La OTAN combate las narrativas falsas antes de su difusión, informando con hechos a través de redes sociales y su web. Así, EE. UU. y el Reino Unido divulgaron inteligencia previa a la invasión de Ucrania en 2022, neutralizando los pretextos rusos⁵². El Comunicado de Bruselas de 2021 reafirmó la promoción de valores democráticos y la necesidad de amplificar voces creíbles⁵³. Al abordar los mitos sobre sus ejercicios en Europa del Este, la OTAN demuestra que la comunicación proactiva es parte esencial de su estrategia.

El «tercer pilar» es la coordinación con aliados y socios, incluida la cooperación con la UE, el G7 y empresas tecnológicas⁵⁴. A través del Sistema de Alerta Rápida de la UE, la OTAN comparte análisis y buenas prácticas frente a la desinformación. La Cumbre de Vilna de 2023 reforzó esta colaboración, y la iniciativa OTAN 2030 destacó la resiliencia como primera línea de defensa ante amenazas híbridas⁵⁵.

⁴⁹ NATO. *NATO's Approach...*, 2023.

⁵⁰ HEADS OF THE STATES AND GOVERNMENTS OF THE NATO ALLIES. *NATO 2022 Strategic Concept*. Madrid (España), NATO STRATCOM, 2022, p. 4. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

⁵¹ NATO. *NATO's Approach...*, 2023.

⁵² DEVLIN, Kayleen, HORTON, Jacob y ROBINSON, Olga. «Ukraine Crisis: Is Russia Staging “False Flag” Incidents?», *BBC News*. 23 de febrero de 2022. Disponible en: <https://www.bbc.com/news/60470089>.

⁵³ HEADS OF THE STATES AND GOVERNMENTS OF THE NATO ALLIES. *Brussels Summit Communiqué Issued*. NATO, 14 de junio de 2021. Disponible en: https://www.nato.int/cps/en/natohq/news_185000.htm.

⁵⁴ NATO. *NATO's Approach...*, 2023.

⁵⁵ HEADS OF THE STATES AND GOVERNMENTS OF THE NATO ALLIES. *Vilnius Summit Communiqué*. NATO, 7 de noviembre de 2023. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

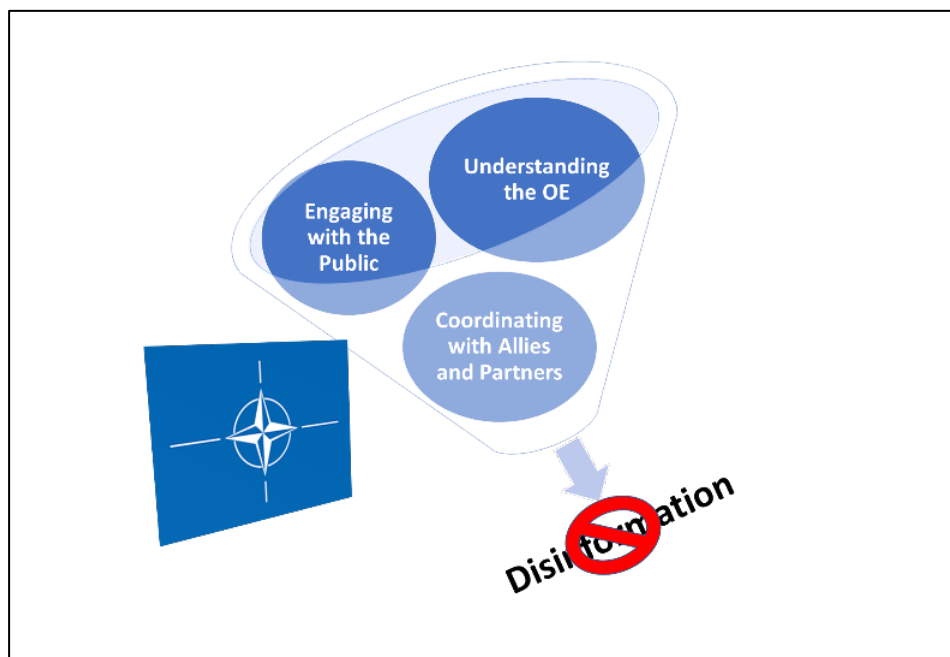


Imagen 4. La estrategia de la OTAN. Creada por el autor

En resumen, la estrategia de la OTAN refleja una cultura estratégica defensiva basada en la conciencia situacional, la comunicación proactiva y la cooperación. Este enfoque integral demuestra su compromiso con la transparencia, la resiliencia y los valores democráticos, y sirve de base para futuras recomendaciones políticas frente a la desinformación rusa. Sin embargo, al igual que la estrategia de la UE, sigue siendo insuficiente.

Prospectiva

La UE y la OTAN afrontan un desafío creciente ante la desinformación rusa, una amenaza sofisticada que erosiona la confianza pública y los valores democráticos. Sus estrategias requieren mayor coherencia y coordinación, avanzando hacia un enfoque conjunto de toda la alianza y toda la sociedad. Basado en el modelo «preparar, actuar y aprender» de Pamment *et al.*, este enfoque propone integrar educación, alfabetización mediática,

comunicación estratégica e innovación tecnológica para construir una defensa proactiva y resiliente⁵⁶.

La «preparación» es esencial para fortalecer la resiliencia institucional y social. La alfabetización mediática, la concienciación y la formación crítica permiten identificar la manipulación emocional y los sesgos cognitivos que sustentan la desinformación. Centros como el Hybrid Center of Excellence (CoE), Strategic Communication (StratCom) CoE y el Baltic Center for Media Excellence deben coordinarse con universidades y diversas ONG para desarrollar programas específicos y herramientas de detección basadas en inteligencia artificial. Un marco estratégico y legislativo común permitirá anticipar amenazas y reforzar las defensas sociales.

Una respuesta efectiva exige «actuar» mediante una coordinación multinivel frente a campañas activas y sus canales de difusión. La armonización de narrativas militares y civiles refuerza la credibilidad institucional y contrarresta la propaganda de actores estatales y sus *proxies*. Las herramientas de verificación automática y las alianzas público-privadas deben combatir *bots* y amplificadores encubiertos, promoviendo contenidos fiables y rompiendo burbujas informativas. A su vez, los marcos legales deben disuadir la producción y distribución de desinformación, todo ello sin comprometer los principios democráticos.

«Aprender» mediante una evaluación constante de campañas pasadas permite mejorar las respuestas futuras. Documentar narrativas hostiles —como las anti-LGTBQ+ en Europa del Este— facilita detectar vulnerabilidades y diseñar contracampañas adaptadas. La inteligencia artificial y la aplicación de técnicas de análisis de *big data* ayudan a identificar patrones de manipulación y sesgos explotados. Fomentar la transparencia y el debate público mediante líderes e influenciadores refuerza la confianza social y reduce la exposición a la manipulación digital.

En general, defenderse de la desinformación rusa requiere una estrategia integral, tecnológica y adaptativa que combine la capacidad institucional de la OTAN y la UE con la resiliencia de la sociedad civil. La preparación fortalece las defensas, la acción coordinada garantiza respuestas efectivas y el aprendizaje continuo asegura la adaptación

⁵⁶ PAMMENT, James *et al.* *Countering Information Influence Activities: The State of the Art*. Research Report Version 1.4. Lund (Suecia), Department of Strategic Communication, Lund University, 2018, pp. 85–86. Disponible en: <https://rib.msb.se/filer/pdf/28697.pdf>.

frente a amenazas cambiantes. Este enfoque conjunto permitirá proteger los valores democráticos y consolidar una defensa sostenible frente al marco estratégico ruso de desinformación.

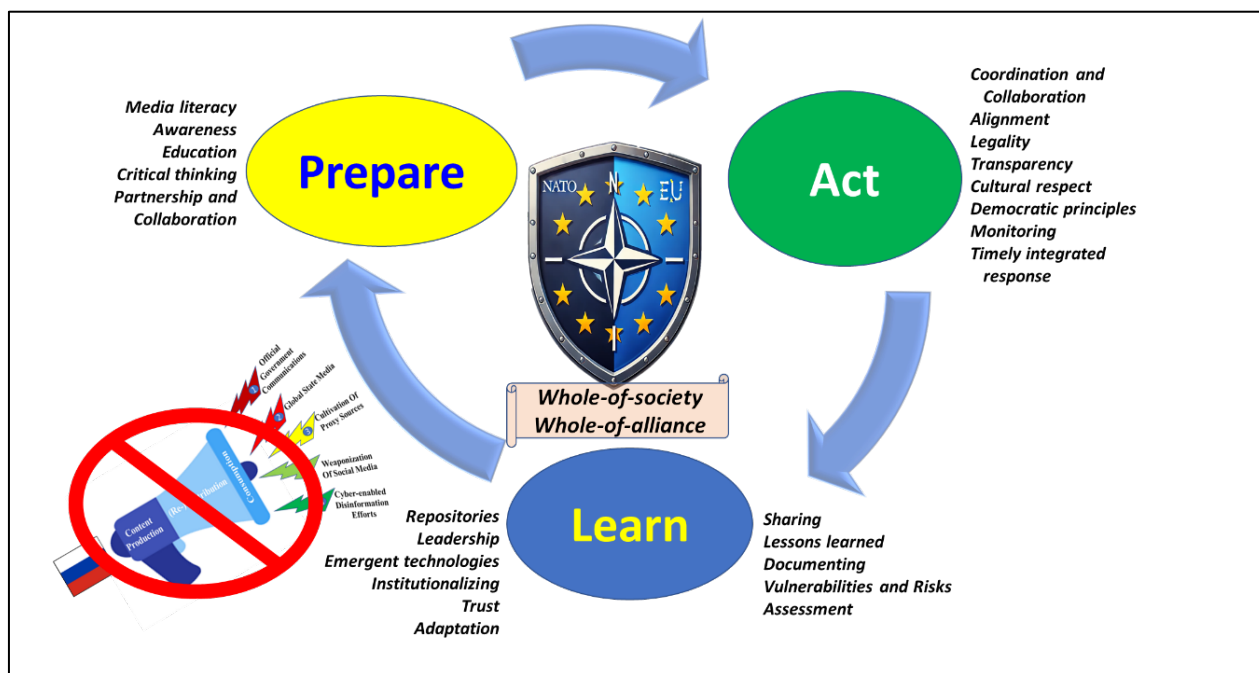


Imagen 5. La estrategia propuesta. Creada por el autor

Conclusiones

La desinformación rusa funciona mediante la combinación de volumen, velocidad y variabilidad: repite hasta generar ilusión de verdad, explota sesgos y crisis, y oculta incoherencias. Contrarrestarla exige anticipación psicológica (*pre-bunking*), fricción algorítmica a la repetición, verificación lateral sostenida, protocolos de crisis con desclasificación rápida y formación en sesgos. Este enfoque convierte el diagnóstico en ventaja operativa.

El modelo ruso es triádico y está apoyado en cinco pilares —comunicaciones oficiales, medios estatales, *proxies*, redes sociales y ciberespacio— con fabricación, contradicción calculada y segmentación. Degradarlo implica actuar en toda la cadena: producción y *proxies* (*pre-bunking* y sanciones), distribución (frenar repetición, retirar *bots* y *astroturfing*, auditar plataformas) y consumo (inoculación narrativa, prioridad a verificadores y

portavoces). Al integrarse en células conjuntas de la UE–OTAN de respuesta rápida, reduciría la superficie de ataque y aumentaría los costes del adversario.

La evidencia (Países Bajos) muestra un patrón estable: amplificación coordinada, bulos y explotación emocional, con efectos de verdad ilusoria, confirmación y erosión de confianza. La respuesta requiere ciclos continuos de vulnerabilidad-contingencia, acuerdos con plataformas para cortar o limitar la repetición de desinformación y redes estables de *pre-bunking* y verificación con KPI de detección, retirada y alcance.

La UE y la OTAN aportan capacidades complementarias: la UE regula (moderación transparente, auditorías, priorización de información fiable), y la OTAN añade alerta situacional y coordinación aliada. Para cerrar brechas se requiere ejercer un mando y control conjunto, *playbooks* comunes, *pre-bunking* paneuropeo con métricas bien definidas, auditorías técnicas a plataformas y formación generalizada en resiliencia cognitiva a toda nuestra sociedad.

El futuro depende de un ciclo permanente «preparar–actuar–aprender». Preparar implica elevar el umbral cognitivo con alfabetización, pensamiento crítico y coordinación entre centros de excelencia y sociedad civil. Actuar supone sincronizar narrativas, alianzas público-privadas y degradación técnica de *bots* y *astroturfing* sin dañar derechos fundamentales. Aprender implica un análisis continuo de narrativas hostiles, técnicas de *big data* para identificar y desenmascarar los patrones y un liderazgo basado en la transparencia. Operativizar este ciclo mediante una célula conjunta constituida por la UE y la OTAN, ejercicios periódicos y KPI compartidos permitirá pasar de reacción fragmentada a prevención sistemática y blindar los valores democráticos.

La verdad es el terreno decisivo del siglo XXI: no defenderla no es neutralidad, es capitulación estratégica.

Eduardo Lobo Almazán

Comandante de Transmisiones del Ejército de Tierra.
Graduado en Psicología, DEM y graduado del US-Army CGSC y SAMS