Opinion Paper

26/2026 06/03/2026

Eduardo Lobo Almazán

War for the Truth: Anatomy and Defense Against Russian Disinformation

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.

Keywords:

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

How to quote:

LOBO ALMAZÁN, Eduardo. *War for the Truth: Anatomy and Defense Against Russian Disinformation*. Opinion Paper. IEEE 26/2026. web link IEEE and/or link bie[3] (accessed on the web day/month/year)

Introduction

The war for the truth is no longer decided in offices, but in the minds of citizens. The Russian "*Firehose of Falsehood*" model turns repetition, availability, and confirmation bias into precision ammunition: a multichannel avalanche that exploits emotion, distraction, and information bubbles to colonize the agenda. This article shows that psychological engineering—from the illusory truth effect to the sleeper effect—and explains why even contradictory messages gain traction when the source is perceived as authoritative.

Russia does not issue isolated messages: it operates an industrial ecosystem—*production, distribution, and consumption*—that manufactures narratives, amplifies them through proxies and bots, and inserts them into segmented audiences to maximize polarization and institutional erosion. The disinformation value chain is analyzed—from defamation and strategic contradiction to amplification and targeted consumption—to understand an influence that is rapid, flexible, and difficult to attribute.

The 21st century has turned disinformation into a strategic vector: Russia exploits the fissures within NATO and EU democracies to polarize, delegitimize institutions, and influence democratic elections. The case of the Netherlands shows how a manufactured narrative—Euroscepticism, fabricated videos, “zombie” accounts, emotional framing—penetrates public debate and displaces reality. These examples offer an operational analysis of such campaigns to identify levers for resilience and electoral protection.

Europe has built a dual architecture to counter disinformation: a regulatory EU that combines self-regulation (2018/2022 Codes) and hard law (DSA), and an operational NATO that structures situational awareness and public engagement through multilevel coordination. This section contrasts the normative and operational models and explains how they complement each other to protect the information ecosystem without undermining freedoms.

Finally, the article moves from diagnosis to prescription with a whole-of-alliance and whole-of-society approach, anchored in the *Prepare–Act–Learn cycle*: education, media literacy, interoperable strategic communication, technological innovation, and EU–NATO regulatory coherence to shift from delayed reaction to systematic prevention.

Disinformation

The first step in designing an effective strategy against disinformation is understanding the threat. The Russian propaganda model, known as the "*Firehose of Falsehood*," is effective because it manipulates psychological biases and heuristics that make it difficult to distinguish truth from falsehood.[1] Psychology explains why this approach succeeds in shaping public opinion and influencing behavior.

Russia spreads *a flood of content across multiple platforms*, increasing the likelihood that its narratives will be internalized. Based on selective exposure, this method exploits repetition and the availability heuristic: the more a message is repeated, the more credible it seems. Familiarity reduces critical thinking, and confirmation bias strengthens the impact when the message aligns with prior beliefs.

This model *disseminates information quickly, continuously, and repetitively*. Constant repetition triggers the illusory truth effect, in which repeated statements are perceived as true, especially among passive audiences. Cognitive biases, first impressions, and information bubbles reinforce prior beliefs and isolate individuals from alternative viewpoints. Repeating falsehoods reduces their perceived immorality and facilitates their spread.

Russian propaganda *ignores the objective truth and exploits various psychological biases*. The sleeper effect explains how people remember the message but forget its source, which prolongs its impact.[2] Combined with confirmation bias, this encourages acceptance of narratives that fit pre-existing beliefs, reducing cognitive dissonance.[3] Appealing to emotions such as fear or anger, it reinforces existing ideologies and perceptions.[4] In contexts of crisis and uncertainty, when official messages are unclear,

---

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

[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, June 1998, p. 211. Available in: 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, nº 2, March 2015, pp. 145 y 155. Available in: https://doi.org/10.1177/1745691615569849.

disinformation spreads more effectively, as demonstrated during the COVID-19 pandemic.[5] This strategy maximizes its effect by exploiting the public's emotional and cognitive vulnerability.

Lastly, Russian propaganda is *inconsistent*. This inconsistency also reinforces its impact. Although it contradicts the repetition principle, it can stimulate public interest and curiosity, thereby increasing perceived credibility.[6] This was observed in the shifting messages about Malaysia Airlines Flight MH17.[7] Similarly, in the case of the annexation of Crimea (2014), President Putin's inconsistent narratives illustrate how inconsistency does not necessarily undermine influence when peripheral cues—such as the perceived authority of the source—enhance credibility.[8] This flexibility allows narratives to be adapted to the Kremlin's strategic objectives, maintaining credibility through outlets like *RT* and *Sputnik*.[9]

In summary, the Russian disinformation model relies on exploiting psychological heuristics that monopolize attention, shape beliefs, and sustain influence even when messages are false or contradictory. Understanding these mechanisms is essential for designing effective detection and defense strategies.

A Regional Approach: The Case of Russia

Russian disinformation operates as an ecosystem composed of three parts: *production, distribution, and consumption*.[10] It manipulates information, spreads it through adapted dissemination techniques, and targets diverse audiences to influence their perceptions.

---

[5] DEPARTAMENTO DE SEGURIDAD NACIONAL, Gobierno de España, *Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional: Trabajos 2023*. Madrid (Spain): Consejo de Seguridad Nacional, 2023, p. 18. Available in: 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 Zakary L. TORMALA, *When Contradictions Foster Persuasion: An Attributional Perspective*. Journal of Experimental Social Psychology, vol. 49, nº 3, May 2013, pp. 426 y 438. Available in: 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., Richard E. PETTY, y Pablo BRIÑOL, *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, April 2008, pp. 147–148. Available in: 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. Available in: https://www.rand.org/pubs/research_reports/RR3160.html.

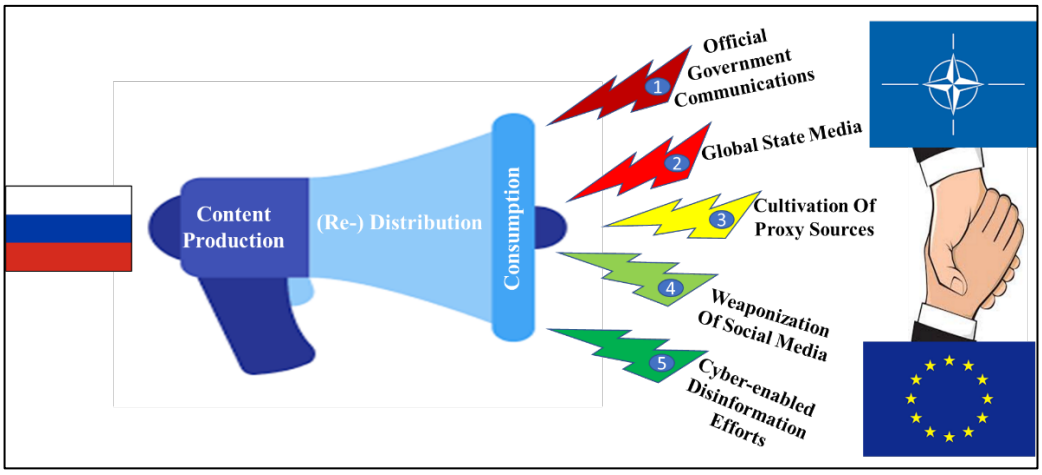

Figure 1. Model of the Pathology of Russian Malign/Subversive Information Efforts. Created by the author.

Regarding the *production phase*, Russian disinformation campaigns create and manipulate information to achieve strategic goals, defaming governments, non-governmental actors, and policies while fostering discord and promoting actors aligned with Moscow.[11] In the 2017 French elections, Russian media accused Emmanuel Macron of being a "US agent," using antisemitic tropes to undermine his credibility and polarize the electorate.[12] This incited political action from right-wing conspiracy theorists and exploited social divisions.

At the same time, Russia amplifies positive narratives about its identity, culture, institutions, and achievements, appealing to historical ties with its audiences and using major international events to project power.[13] For example, Russia glorifies its international events to project strength and deflect criticism.[14]

To sow confusion, it generates and spreads contradictory versions, as seen in the case of the poisoning of Sergei Skripal, creating uncertainty and distrust.[15] Through state

[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*. 2nd of April 2017. Available in: https://sputnikglobe.com/20170204/macron-us-agent-dhuicq-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. Available in: 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 Media" – Journalist*. 18 July 2018. Available in: https://sputnikglobe.com/20180718/russia-world-cup-mainstream-media-1066453434.html.
[15] JOSHI, Shashank, *Skripal: The Weight of Evidence*. The Interpreter, 5th of April 2018. Available in: https://www.lowyinstitute.org/the-interpreter/skripal-weight-evidence;
MATTHEWS, Miriam *et al., Understanding and Defending…*, 2021, p. 20.

media and bots, messages were disseminated that discredited European authorities with the aim of weakening Euro-Atlantic cohesion.[16]

Content production involves fabrication, distortion, and selective use of facts, exploiting emotion and confusion as tools of global influence.[17]

Regarding *distribution*, Russia disseminates its disinformation through a diverse network of actors and channels tailored to each context.[18] State-controlled media outlets like *RT* and *Sputnik* openly spread manipulated content to shape global perceptions in favor of the Kremlin.[19]

Other actors, such as the *Internet Research Agency* (IRA) or WikiLeaks, operate as intermediaries with opaque ties.[20] For example, during the 2016 US elections, they effectively used fake profiles to spread divisive messages and weaken Hillary Clinton, aligning with Russia's strategic interests.[21]

Similarly, unaffiliated figures and media outlets—including influencers with extreme ideologies in Europe and the US—may unintentionally amplify Russian narratives, sometimes with covert funding. Right-wing influencers like Benny Johnson, Tim Pool, and Dave Rubin are non-state actors who unknowingly took part in Russian influence operations when Russian state media covertly funded their English-language videos promoting pro-Russian viewpoints.[22]

---

[16] JEANGÈNE VILMER, J.-B. *et al., Information Manipulation: A Challenge for Our Democracies*. Paris (France): 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. Available in: 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 Samuel ROBERTSHAW, *Weaponising News: RT, Sputnik, and Targeted Disinformation*. London (United Kingdom): Policy Institute, King's College London, 2019, p. 107. Available in: 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. Available in: 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*. London (United Kingdom): I.B. Tauris, 2020, p. 9. Available in: 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] LYNGAAS, Sean y Jonathan PASSATINO, *Right-Wing Influencers Say They Were Dupes in an Alleged Russian Influence Operation. They Are Keeping Their Millions for Now*. CNN, 13 September 2024. Available in: https://www.cnn.com/2024/09/13/media/right-wing-media-influencers-tenet-russian-money/index.html; SUDERMAN,

Russia uses traditional media, digital platforms, and social networks as primary channels to reach its target audiences. [23] Examples include misleading messages from the Russian Ministry of Foreign Affairs on *Twitter* (now *X*) after the Skripal case, or the mass dissemination of content by *RT* and *YouTube*. [24] Additionally, forums organized by proxies and official statements reinforce this strategy.[25]

Taken together, the multiplicity of actors and platforms enables Russia to effectively disseminate disinformation, obscure its origins, and create the appearance of spontaneous movements aligned with its strategic interests.

Finally, the *consumption* of Russian disinformation constitutes the last phase of the ecosystem. Target audiences absorb content designed to manipulate public opinion and reinforce polarization. Russia tailors its messages toward specific demographic groups through cultural, historical, and political narratives that reinforce biases and institutional distrust.

Its reach includes the general public, elites, and influencers.[26] In Europe, it exploits both the far right and the far left with anti-Western and anti-establishment messages, generating echo chambers that amplify discord and undermine trust in NATO and the EU.[27] The 2020 US elections illustrate this dynamic: Russian interference sought to weaken Joe Biden through troll farms and social media networks controlled by the IRA, repeating tactics already used in 2016 to divide and suppress voter turnout.[28]

Alan, y Alison SWENSON, *Right-Wing Influencers Were Duped to Work for Covert Russian Operation, US Says*. Associated Press**,** September 2024. Available in: https://apnews.com/article/russian-interference-presidential-election-influencers-trump-999435273dd39edf7468c6aa34fad5dd.

[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 March 2018. Available in: 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. Available in: 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, June 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, February 2020. Available in: 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.

Russia also appeals to cultural, religious, and historical ties. Narratives such as anti-LGBTQ+ messaging resonate in Eastern Europe, where Moscow is portrayed as a defender of traditional values against a decadent "*Gayropa*."[29]

The use of bots, astroturfing, automated accounts, and algorithm manipulation on social media amplifies the dissemination of misinformation.[30] This creates a human-like appearance for the messages, as was evident in the U.S. in both 2016 and 2020. Bots flooded platforms with divisive content, expanding their reach and drawing in unsuspecting audiences, whose engagement further legitimized the messages.[31]

Russia's methods are adapted to the media environment: traditional media in the East, social networks in the West.[32] Their effectiveness varies; in pro-Russian regions, such as Hungary, where local media openly replicate Russian narratives, they have a significant impact.[33] In less receptive areas, covert methods are required to simulate support.[34] Nevertheless, in the Baltic states and Finland, audiences largely reject these messages, as reflected in declining support for Soviet symbols—evidenced by decreased participation in May 9th celebrations, the date of Soviet victory over Germany.[35]

Clearly, Russia's disinformation machinery operates through a sophisticated ecosystem of *production, distribution, and consumption*, built on five key pillars: official communications, global state media, proxy sources, social networks, and cyberspace.[36]

---

[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, 29th of June 2024. Available in: 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. Brussels (Belgium): European Parliament, 2021, p. 7. Available in: 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, March 2018, p. 1095. Available in: 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, November 2018, pp. 1–2. Available in: 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 (Hungary): Political Capital, 2016, p. 7. Available in: 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, August 2020, p. 8. Available in: https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

Its structure allows it to project a flexible, decentralized, and hard-to-attribute narrative. State media reinforce these narratives, responding swiftly to political objectives and maintaining a constant focus on discrediting perceived adversaries. And although the EU has sanctioned outlets like RT and Sputnik, Russia adapts through new domains and platforms, exploiting the slower response times of Western democracies.[37] Despite varying results, Russian disinformation remains a strategic tool of Soft Power or Smart Power, eroding social cohesion and challenging global democratic resilience.

A Practical Approach: The 21st Century

Since the end of the Cold War and the rise of Putin, Russian disinformation has targeted NATO and EU countries. Its purpose has been to exploit social divisions, weaken cohesion, polarize politics, and erode alliances to achieve geopolitical objectives. Understanding these campaigns is essential for designing an effective strategy. The case of the referendum held in the Netherlands offers key lessons for strengthening resilience, promoting digital literacy, protecting electoral processes, and balancing countermeasures with democratic values.

The 2016 Dutch referendum on the EU–Ukraine Association Agreement exemplifies how Russia exploited Euroscepticism to influence public opinion. Through outlets such as *RT* and *Sputnik*, it amplified narratives portraying Ukraine as corrupt and dependent, spreading falsehoods like the alleged crucifixion of a child and manipulated videos showing Azov Battalion soldiers burning a Dutch flag.[38] Although Bellingcat debunked this content and linked it to the IRA, the campaign supported Russia's efforts by portraying Ukraine as a threat to European stability.[39]

---

[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, series L, n.º 65, February 2022, pp. 6–7. Available in: 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, series L, n.º 190 I, July 2023, pp. 21–27. Available in: 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, section World, Nueva York (NY), 16 February 2017. Available in: 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, 03 April 2016. Available in: https://www.bellingcat.com/news/uk-and-europe/2016/04/03/azov-video; DELOY, Corinne y Pascale JOANNIN, *The Dutch Reject the Association Treaty between the EU and Ukraine*.

Figure 2. Fabricated image of Azov fighters burning a Dutch flag.[40]

Russia also capitalized on local Eurosceptic movements. The blog *GeenStijl* echoed anti-EU rhetoric and Putin's narratives, describing the agreement as a threat to Russian sovereignty and European identity as a product of the Euromaidan, while labeling the Ukrainian government as neo-Nazi.[41] Political figures such as Harry van Bommel (a left-wing MP) and Thierry Baudet (leader of the Forum for Democracy party) amplified these messages. They lent them legitimacy and contributed to the rejection of the agreement.[42]

The Dutch case demonstrates how Russia employs psychological biases such as the illusory truth effect and selective exposure to reinforce anti-EU and anti-Ukrainian prejudices. Through contradictory narratives and tailored messaging, the Kremlin aligned its efforts with the Russian Strategic Disinformation Model described earlier, fueling confusion and distrust toward the EU.

The lessons from the referendum highlight the need to adopt comprehensive measures to counter disinformation, including vulnerability assessments, contingency plans, legal frameworks, and civic education. Strengthening resilience also requires training political parties, protecting the media, cooperating with digital platforms, and promoting

Policy Paper 388, European Issues. Paris (France): Foundation Robert Schuman, 2016, p. 2. Available in: 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 March 2016. Available in: https://www.greeneuropeanjournal.eu/the-dutch-ukraine-referendum-between-apathy-and-antipathy.

[42] HIGGINS, *Fake News, Fake Ukrainians…*, 2017.

international collaboration on best practices.[43]

A Strategic Approach: The EU and NATO

The EU addresses disinformation through a mixed approach that combines voluntary self-regulation with mandatory legislation, aiming to protect the European information environment without infringing on fundamental rights such as freedom of expression.

Its framework is based on *the Code of Practice on Disinformation* (2018) and its *strengthened version* (2022), as well as the *Digital Services Act* (DSA, 2022).[44] The voluntary codes recommend that platforms like *Meta*, *Google*, *X*, and *TikTok* demonetize disinformation, ensure transparency in political advertising, and support fact-checkers and researchers.[45] The strengthened code expanded these commitments to 44 measures, creating a transparency center and prioritizing media literacy, the removal of fake accounts, and the promotion of reliable information.

The DSA, in turn, imposes binding obligations on digital platforms—especially very large ones—regarding content moderation, advertising transparency, and risk management through independent audits. Its goal is to ensure a safe, predictable digital space that respects the EU Charter of Fundamental Rights.

In addition, the EU has responded to specific threats such as Russian disinformation. It banned *RT* and *Sputnik* broadcasts following the invasion of Ukraine and, in 2022, supported the creation of the European Fact-Checking Standards Network (EFCSN), which brings together 45 outlets from 30 countries under a common ethical code.[46]

---

[43] BRATTBERG, Erik, y Timothy MAURER, *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. Available in: 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*. Brussels (Belgium): European Commission, 2018. Available in: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation; EUROPEAN COMMISSION, *2022 Strengthened Code of Practice on Disinformation*. Brussels (Belgium): European Commission, 2022. Available in: 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, series L 277, October 2022, pp. 1–102.

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

[46] EUROPEAN FACT-CHECKING STANDARDS NETWORK (EFCSN), *Frequently Asked Questions. What Is the EFCSN?* European Fact-Checking Standards Network (EFCSN), consulted on 27 September 2024. Available in: https://efcsn.com.

Finally, the proposed *Artificial Intelligence Act* (2021) reinforces this commitment by requiring AI-generated content to be clearly identifiable and by adapting regulation to new technological challenges.[47]

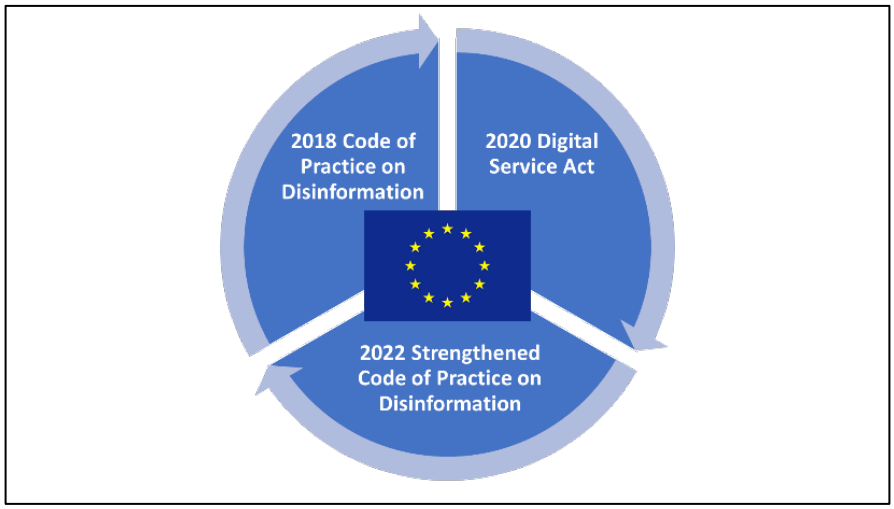

Figure 3. The EU's current strategy. Created by the author.

In summary, the EU's strategy against disinformation is evolving in cycles—from self-regulation in 2018 to full regulation under the DSA—continuously refining its tools to strengthen transparency, trust, and the integrity of the European information ecosystem. Nevertheless, as disinformation continues to cause harm, this strategy remains insufficient.

Although there is no single document, *NATO's strategy against disinformation* is based on a dual-track model focused on understanding and engagement, reinforced by various strategic elements that enhance its capacity to address information warfare in today's security environment.[48]

The first pillar is understanding the information environment.[49] Through its assessment capabilities, NATO continuously analyzes sources of disinformation, hostile narratives, and emerging behaviors. *The 2022 Strategic Concept*, adopted at the *Madrid Summit*, identifies Russia as a key actor and emphasizes the need to counter hybrid tactics.[50]

[47] DEPARTAMENTO DE SEGURIDAD NACIONAL, *Foro contra las Campañas de Desinformación …*, 2023, p. 25.
[48] NATO, *NATO's Approach to Countering Disinformation*. NATO, November 2023. Available in: https://www.nato.int/cps/en/natohq/topics_219728.htm.
[49] NATO, *NATO's Approach…*, 2023.
[50] HEADS OF THE STATES AND GOVERNMENTS OF THE NATO ALLIES, *NATO 2022 Strategic Concept*. Madrid

Concrete examples include: the UK's Rapid Response Unit, which detects Russian campaigns; the Lithuanian Armed Forces, which monitor propaganda; and the US Office of the Director of National Intelligence, which lists Russia among the top threats.

The second pillar is public engagement, based on transparent and anticipatory communication (pre-bunking).[51] NATO counters false narratives before they spread, sharing factual information via social media and its website. For example, the US and the UK released intelligence ahead of Russia's 2022 invasion of Ukraine, neutralizing Russian pretexts.[52] *The 2021 Brussels Communiqué* reaffirmed the promotion of democratic values and the need to amplify credible voices.[53] By addressing myths about its exercises in Eastern Europe, NATO shows that proactive communication is a key part of its strategy.

The third pillar is coordination with allies and partners, including cooperation with the EU, the G7, and tech companies.[54] Through the EU's Rapid Alert System, NATO shares analyses and best practices to combat disinformation. *The 2023 Vilnius Summit* reinforced this collaboration, and *the NATO 2030 initiative* highlighted resilience as the first line of defense against hybrid threats.[55]

(Spain): NATO STRATCOM, 2022, p. 4. Available in: 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, Jacob HORTON, y Olga ROBINSON, *Ukraine Crisis: Is Russia Staging "False Flag" Incidents?* BBC News, 23 February 2022. Available in: https://www.bbc.com/news/60470089.

[53] HEADS OF THE STATES AND GOVERNMENTS OF THE NATO ALLIES, *Brussels Summit Communiqué Issued*. NATO, 14 June 2021. Available in: 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 November 2023. Available in: https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

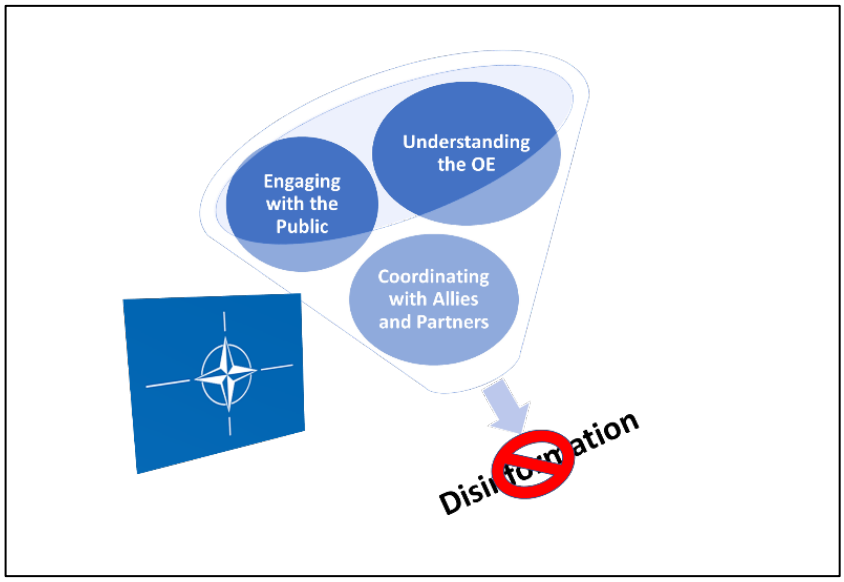

Figure 4. NATO´s current strategy. Created by the author.

In essence, NATO's strategy reflects a defensive strategic culture based on situational awareness, proactive communication, and cooperation. This comprehensive approach demonstrates its commitment to transparency, resilience, and democratic values, and serves as a foundation for future policy recommendations to counter Russian disinformation. Nonetheless, like the EU's strategy, it remains insufficient.

Foresight

The EU and NATO face a growing challenge from Russian disinformation—a sophisticated threat that erodes public trust and democratic values. Their strategies require greater coherence and coordination, moving toward a joint *whole-of-alliance* and *whole-of-society approach*. Based on the *Prepare, Act, and Learn model* by Pamment et al., this approach proposes integrating education, media literacy, strategic communication, and technological innovation to build a proactive and resilient defense.[56]

Preparation is essential for strengthening institutional and social resilience. Media literacy, awareness, and critical training enable individuals to recognize emotional manipulation and the cognitive biases that underpin disinformation. Centers such as *the Hybrid Center of Excellence (CoE), the Strategic Communication (StratCom) CoE,* and

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

the Baltic Center for Media Excellence should coordinate with universities and NGOs to develop targeted programs and AI-based detection tools. A common strategic and legislative framework will help anticipate threats and reinforce social defenses.

An effective response requires coordinated action across multiple levels against active campaigns and their dissemination channels. Harmonizing military and civilian narratives strengthens institutional credibility and counters propaganda from state actors and their proxies. Automatic verification tools and public-private partnerships must combat bots and covert amplifiers, promote reliable content, and break information bubbles. At the same time, legal frameworks must deter the production and distribution of disinformation—without compromising democratic principles.

Learning from constant evaluation of past campaigns enables improved future responses. Documenting hostile narratives—such as anti-LGBTQ+ messaging in Eastern Europe—helps identify vulnerabilities and design tailored counter-campaigns. Artificial intelligence and the application of Big Data analysis techniques help detect manipulation patterns and exploited biases. Promoting transparency and public debate through leaders and influencers strengthens social trust and reduces exposure to digital manipulation.

Overall, defending against Russian disinformation requires a comprehensive, technological, and adaptive strategy that combines NATO and EU institutional capacity with the resilience of civil society. *Preparation* strengthens defenses, *coordinated action* ensures effective responses, and continuous *learning* enables adaptation to evolving threats. This joint approach will help protect democratic values and build a sustainable defense against Russia's strategic disinformation framework.

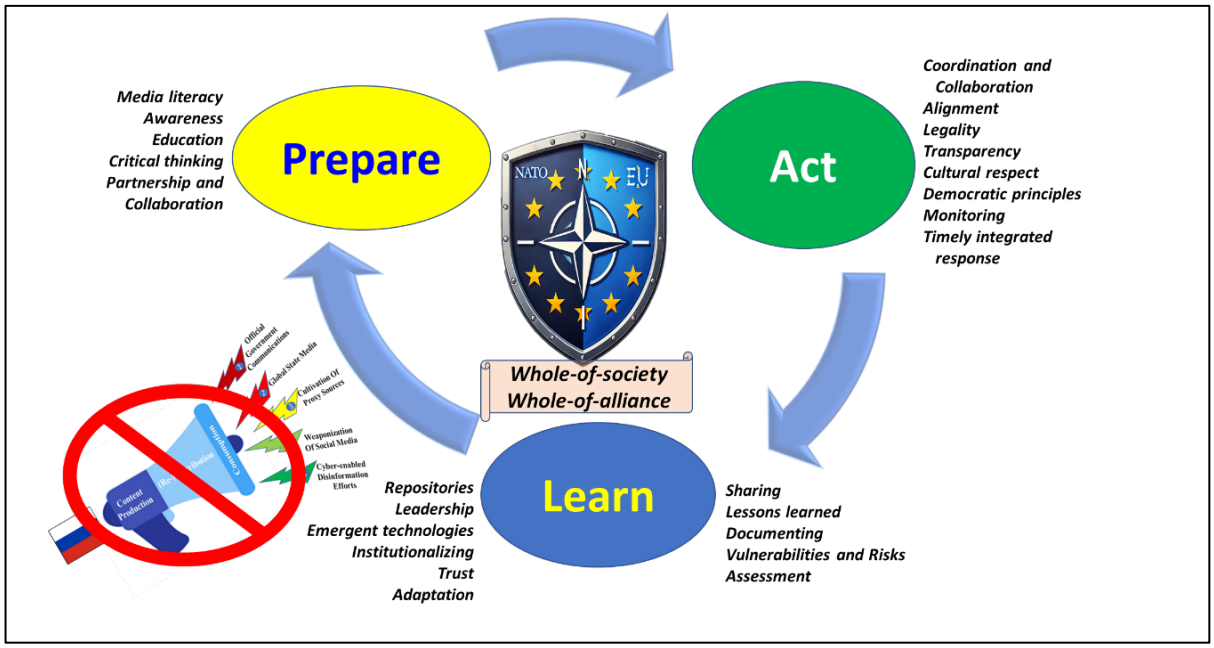

Figure 5. The proposed strategy. Created by the author.

Conclusion

Russian disinformation operates through a combination of volume, speed, and variability: it repeats messages until they create an illusion of truth, exploits biases and crises, and conceals inconsistencies. Countering it requires psychological anticipation (pre-bunking), algorithmic friction against repetition, sustained lateral verification, crisis protocols with rapid declassification, and training in cognitive biases. This approach turns diagnosis into an operational advantage.

The Russian model is triadic and supported by five pillars—official communications, state media, proxies, social networks, and cyberspace—based on fabrication, calculated contradiction, and segmentation. Degrading it requires action across the entire chain: production and proxies (pre-bunking and sanctions), distribution (disrupt repetition, remove bots and astroturfing, audit platforms), and consumption (narrative inoculation, prioritizing fact-checkers and trusted spokespersons). Integrated into EU–NATO joint rapid response cells, this would reduce the attack surface and increase the adversary's costs.

Evidence (e.g., the Netherlands) reveals a consistent pattern: coordinated amplification, falsehoods, and emotional exploitation, with illusory truth effects, confirmation bias, and trust erosion. The response must involve ongoing cycles of vulnerability-contingency,

agreements with platforms to cut or limit the repetition of disinformation, and stable networks for pre-bunking and verification, with KPIs for detection, removal, and reach.

The EU and NATO bring complementary capabilities: the EU regulates (transparent moderation, audits, prioritization of reliable information), while NATO adds situational awareness and allied coordination. Closing the gaps requires joint command and control, shared playbooks, pan-European pre-bunking with clear metrics, technical audits of platforms, and widespread training in cognitive resilience across society.

The future depends on a permanent *Prepare–Act–Learn cycle*. *Prepare* means raising the cognitive threshold through literacy, critical thinking, and coordination between centers of excellence and civil society. The *act* requires synchronizing narratives, public-private partnerships, and technical measures to degrade bots and astroturfing without harming fundamental rights. *Learn* means continuously analyzing hostile narratives, using Big Data techniques to uncover patterns, and promoting leadership grounded in transparency.

Truth is the decisive battleground of the 21st century: not defending it is not neutrality—it is strategic capitulation.

Eduardo Lobo Almazán
Major (ESP-Army), SC, BA in Psychology, US Army CGSC and SAMS Graduate