Cuadernos Europeos de Deusto

No. 74/2026

DOI: https://doi.org/10.18543/ced7420256

ESTUDIOS

Saint George and The New Dragon: the fight of the European Union against disinformation sponsored by foreign states

San Jorge y El Nuevo Dragón: la lucha de la Unión Europea contra la desinformación patrocinada por estados extranjeros

Carlos Espaliú Berdud

doi: https://doi.org/10.18543/ced.3484

Received on January 20, 2026 • Accepted on February 9, 2026 • E-published: May 2026

Derechos de autoría y de explotación

Los autores conservan sus derechos de autor sobre los trabajos publicados en Cuadernos Europeos de Deusto (CED). Además, pueden disponer de sus publicaciones para depositarlas en repositorios, páginas web personales, cursos o como base para futuras publicaciones, siempre que se cite adecuadamente la fuente original. Al enviar un artículo para su revisión y publicación en CED, los autores ceden a la Universidad de Deusto derechos de explotación, incluyendo distribución, comunicación pública, reproducción e inclusión en cualquier tipo de soporte, en particular en bases de datos en las que esta revista está indexada y en el repositorio institucional de la Universidad de Deusto. Los autores garantizan que no se han otorgado ni se otorgarán permisos o licencias de cualquier tipo que puedan violar los derechos otorgados a la Editorial. CED es una revista de acceso abierto, lo que garantiza el acceso gratuito, inmediato y permanente al contenido digital de todos sus números. Los lectores pueden leer, descargar, copiar, distribuir, imprimir, buscar o enlazar los textos completos sin fines comerciales y sin necesidad de autorización previa, siempre que se cite adecuadamente el trabajo original. Cualquier otro uso de su contenido en cualquier medio o formato, ahora conocido o desarrollado en el futuro, requiere el permiso previo por escrito del titular de los derechos de autor. En particular, no se podrán aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras personas a hacer cualquier uso permitido por esta licencia.

Copyright and exploitation rights

Authors retain their copyright on works published in Cuadernos Europeos de Deusto (CED). Moreover, they may make their publications available for deposit in repositories, personal websites, courses or as a basis for future publications, provided that the original source is properly cited. By submitting an article for review and publication in CED, authors grant the University of Deusto exploitation rights, including distribution, public communication, reproduction and inclusion in any type of medium, particularly in databases in which this journal is indexed and in the institutional repository of the University of Deusto. Authors guarantee that no permissions or licences of any kind have been or will be granted that may violate the rights granted to the Publisher. CED is an open access journal, which guarantees free, immediate and permanent access to the digital content of all its issues. Readers may read, download, copy, distribute, print, search or link to the full texts for non-commercial purposes and without prior authorisation, provided that the original work is properly cited. Any other use of its content in any medium or format, now known or developed in the future, requires the prior written permission of the copyright holder. In particular, no legal terms or technological measures may be applied that legally restrict other persons from making any use permitted by this licence.

Saint George and The New Dragon: the fight of the European Union against disinformation sponsored by foreign states

San Jorge y El Nuevo Dragón: la lucha de la Unión Europea contra la desinformación patrocinada por estados extranjeros

Carlos Espaliú Berdud
Full Professor of Public International Law and International Relations
Universidad CEU Fernando III, CEU Universities
Research Fellow, Las Casas Institute, Blackfriars Hall, University of Oxford
carlos.espaliuberdud@ceu.es

doi: https://doi.org/10.18543/ced.3484

Received on January 20, 2026
Accepted on February 9, 2026
E-published: May 2026

Summary: I. Introduction.—II. The paper war.—III. The real war. 1. On the EU's response to disinformation campaigns in a context of growing rivalry and foreign hostility. 2. On the possible responses of the EU to disinformation campaigns in a war context.—IV. Conclusion.—V. References.

Abstract: In recent years, disinformation orchestrated by foreign states, particularly Russia, has become a major threat to the fundamental rights of EU citizens, as well as to the vital interests of Member States and the Union itself. In this paper, we have studied the EU's fight against disinformation campaigns orchestrated by third countries. We have seen how it has moved from weak policies and measures to the adoption of robust and rigorous policies and measures, including a system of sanctions against individuals, companies and the media. We also ask ourselves whether the EU could resort to self-defence in the face of disinformation campaigns that amount to armed attacks, and what form such a response might take. We conclude that, although this would be possible in theory, in practice it would be difficult to find cases in which the EU itself suffers disinformation campaigns equivalent to armed attacks without affecting Member States, and it would therefore be difficult to imagine a possible response from the EU.

Keywords: disinformation, European Union, FIMI, human rights, self-defence.

Resumen: *En los últimos años la desinformación orquestada por Estados extranjeros, en particular Rusia, se ha convertido en una amenaza importantísima contra los derechos fundamentales de los ciudadanos de la UE, así como a los intereses vitales de los Estados Miembros y de la propia Unión. En este trabajo hemos estudiado la lucha de la UE contra las campañas de desinformación orquestadas por terceros Estados. Hemos visto cómo se ha pasado de unas políticas*

y unas medidas débiles, a la adopción de políticas y medidas sólidas y rigurosas, incluyendo un régimen sancionador a individuos, empresas y medios de comunicación. Nos preguntamos también por la posibilidad de que la UE recurra a la legítima defensa ante campañas de desinformación que equivalgan a ataques armados y las modalidades en que podría manifestarse esa respuesta. Y llegamos a la conclusión que, aunque en teoría ello sería posible, en la práctica será difícil encontrar casos en los que la UE sufra campañas de desinformación equivalentes a ataques armados en sí misma, sin que afectara a los Estados Miembros y, por tanto, sería difícil imaginar la posible respuesta de la UE.

Palabras clave: *desinformación, Unión Europea, FIMI, derechos humanos, legítima defensa.*

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

I. **Introduction**

The use of false information is inherent in the human condition and has historically been used to manipulate public opinion for political, economic or even military purposes[1]. Today, however, the technological revolution that has taken place around the world has multiplied its danger and scope, making it a serious global risk[2] when it takes on the characteristics of "disinformation campaigns". For us, this new form of "information disorder"[3] can be defined as "[...] the orchestrated dissemination of untrue news or data through any type of communication channel, whether traditional —printed press, radio, television— or horizontal —social networks, etc.— with the intention of gaining an economic, social or strategic advantage or harming rivals, be they individuals, societies, institutions or states"[4]. In this article, I will focus on the international relations and geopolitical landscape, and more specifically on the European Union's (EU) ongoing battle against the disinformation campaigns that it and its Member States are increasingly exposed to from abroad, to the point where it has become almost a plague.

Indeed, the seriousness of the threats cannot be underestimated, as they can often affect the exercise of several fundamental rights that form the basis of our European democracies[5]. For example, the right to free and fair elections, when the disinformation is intended to favour or harm a particular candidate, thereby altering the foreseeable expected result[6]. In other cases, when disinformation relates to a person —in particular political and

---

[1] Ángel Badillo and Félix Arteaga, «*El impacto estratégico* de la *desinformación en España*», *Informe IBERIFIER,* Febrero 2024 (2024): 9. https://media.realinstitutoelcano.org/wp-content/uploads/2024/04/informe-iberifier-el-impacto-estratagico-de-la-desinformacion-en-espana.pdf. See also: Centro Criptológico Nacional, Ministerio de Defensa, «Desinformación en el ciberespacio», BP/13 (2019): 5. https://www.ccn-cert.cni.es/es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/3549-ccn-cert-bp-13-desinformacion-en-el-ciberespacio/file.html.

[2] Chengcheng Shao *et al*., «The spread of low-credibility content by social bots», *Nature Communications* 9, 4787 (2018): 2. https://doi.org/10.1038/s41467-018-06930-7

[3] Claire Wardle and Hossein Derakhshan, «Information disorder. Toward an interdisciplinary framework for research and policymaking», Council of Europe (2017). https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.

[4] Carlos Espaliú-Berdud, «Use of Disinformation as a Weapon in Contemporary International Relations: Accountability for Russian Actions Against States and International Organizations», *Profesional De La información* 32 (4) (2023): 5. https://doi.org/10.3145/epi.2023.jul.02.

[5] In this line see, among others: James Pamment, «The EU's Role in Fighting Disinformation: Taking Back the Initiative», *Policy File*, Carnegie Endowment for International Peace —US (2020): 5-6. https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf.

[6] See, among others, Article 25 of the International Covenant on Civil and Political Rights; Article 3 of the Protocol No. 1, of the European Convention on Human Rights

public figures and journalists— and is intended to harm that person's reputation, it may affect the right to be free from unlawful attacks on one's honour and reputation[7]. Or, if the disinformation is sometimes targeted at particular groups in society —such as women, migrants or certain ethnic groups— and is intended to incite violence, discrimination or hostility, it may violate the right to non-discrimination[8]. Moreover, it also can affect the right to privacy, when personal data is misused with illegal purposes[9].

However, in that regard, it should be noted that the scope and danger of disinformation campaigns have increased due to the difficulty democratic societies face in legally tackling these hostile acts, compared to more clearly offensive behaviours such as armed attacks, terrorist acts, and computer attacks or hacking[10]. Indeed, it is difficult to combat disinformation without at the same time attacking the very principles of democratic States and societies —as we have seen above— such as freedom of expression and opinion, which underpin the fundamental individual rights of nationals and foreigners. As it is firmly rooted in the jurisprudence of the European Court of Human Rights (ECtHR), "freedom of expression, [...] constitutes one of the essential foundations of a democratic society and one of the primary conditions for its progress"[11]. This conception lies so much at the

(ECHR); Articles 39 and 40 of the Charter of Fundamental Rights of the European Union; Articles 10 (3) and 14 (3) of the Treaty on European Union (TEU).

[7] See, among others, Article 17 of the International Covenant on Civil and Political Rights; Article 8 of the ECHR; Articles 1 and 7 of the Charter of Fundamental Rights of the European Union.

[8] See, among others, International Convention on the Elimination of All Forms of Racial Discrimination; Convention on the Elimination of All Forms of Discrimination Against Women; Convention on the Rights of Persons with Disabilities; Article 2 of the Convention on the Rights of the Child; Articles 2(1) and 26, of the International Covenant on Civil and Political Rights; Article 2 (2) of the International Covenant on Economic, Social and Cultural Rights; Article 14 of the ECHR and Article 1 to its Protocol No. 12; Articles 21 and 23 of the Charter of Fundamental Rights of the European Union. For a study of the rights that can be affected by disinformation campaigns, see: Gobierno de España. Presidencia del Gobierno. «Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional. Propuestas de la sociedad civil» (2022): 87-90.

[9] The right to privacy is embodied, among others legal instruments, in Article 8 of the ECHR and Article 17 of the International Covenant on Civil and Political Rights.

[10] In this sense, see: Presidencia del Gobierno. «Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional. Propuestas de la sociedad civil», p. 10. To assess how different types of governments (democratic or authoritarian) and international organisations approach the fight against online disinformation, see the comparative research design made by: Samuel,Cipers, Trisha Meyer and Jonas Lefevere, «Government Responses to Online Disinformation Unpacked», *Internet Policy Review*, vol. 12, no. 4 (2023): 1-19. DOI: 10.14763/2023.4.1736.

[11] European Court of Human Rights. *Case of Castells v. Spain*. 11798/85, Judgment (Merits and Just Satisfaction), Chamber, 23 April 1992. ECLI:CE:ECHR:1992:-0423JUD001179885, par. 42.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

heart of European democracies than, according to the Court of Justice of the European Union in a case in which the Court had to examine the right of an official of the European Commission itself to criticize the EU bodies, the authorities cannot silence opinions, even if they are contrary to the official view[12]. In this vein, to illustrate the difficulties faced by public authorities in the fight against online disinformation, it is worth noting that, according to a decision by the ECtHR, Article 10 of the European Convention on Human Rights (ECHR), which is also part of EU law, and that recognizes the right to freedom of expression,

> "[...] does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful. To suggest otherwise would deprive persons of the right to express their views and opinions about statements made in the mass media and would thus place an unreasonable restriction on the freedom of expression set forth in Article 10 of the Convention"[13].

In addition to possible violations of these individual rights, disinformation campaigns orchestrated by foreign States amount to interference in the internal affairs[14] of EU Member States and the EU itself and there is a tendency to consider them as an element of hybrid war and therefore to amount to a violation of the prohibition of the use of force in international society contained in article 2.4 of the UN Charter. For example, in the 2022 New Strategic Concept of the North Atlantic Treaty Organization (NATO), it is emphasized that authoritarian actors:

> "[…] interfere in our democratic processes and institutions and target the security of our citizens through hybrid tactics, both directly and

---

[12] Court of Justice of the European Union. Judgment of the Court of 6 March 2001, *Bernard Connolly v European Commission*, Case C-274/99 P. ECLI:EU:C:2001:127, para. 43.

[13] European Court of Human Rights. *Case of Salov v. Ukraine***,** 65518/01, Judgment, 6 September 2005. ECLI:CE:ECHR:2005:0906JUD006551801, para. 113. For a development of this matter, see: European Parliament. «The fight against disinformation and the right to freedom of expression». Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 695.445 – July 2021.https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695445/IPOL_STU(2021)695445_EN.pdf; Jan Kudrna, «The possibilities of combating so-called disinformation in the context of the European Union legal framework and of constitutional guarantees of freedom of expression in the European Union Member States», *International Comparative Jurisprudence (Online)* 8.2 (2022): 138–151. https://doi.org/10.13165/j.icj.2022.12.002.

[14] On the possibility to consider influence operations as a violation of State's sovereignty, see: Duncan Hollis, «The Influence of War; The War for Influence», *Temple International and Comparative Law Journal* 32, no. 1 (Spring 2018): 39. https://sites.temple.edu/ticlj/files/2018/10/32.1_Article-5_Hollis.pdf.

> through proxies. They conduct malicious activities in cyberspace and space, promote disinformation campaigns, instrumentalise migration, manipulate energy supplies and employ economic coercion"[15].

NATO had already in 2016 set forth that it could invoke Article 5 of the Washington Treaty in the presence of hybrid warfare, "[...] where a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, are employed in a highly integrated design by state and non-state actors to achieve their objectives [...]"[16].

In the same line, for example, the German «White Paper on Security Policy and the Future of the Bundeswehr 2016» states that: "[...] A special challenge for open and pluralistic societies is the use of digital communication to influence public opinion, for example through hidden attempts to sway discussions on social media and by manipulating information on news portals. This approach has already gained special significance as an element of hybrid warfare"[17]. And it added that: "[...] Hybrid tactics blur the boundaries between war and peace and can also constitute a breach of the general ban on the use of force. The roles of aggressor and conflict party are deliberately obscured. The intention is to delay or completely prevent an immediate and decisive response by the state under attack and the international community"[18].

---

[15] See: North Atlantic Treaty Organization. «2022 Strategic Concept. Adopted by Heads of State and Government at the NATO Summit in Madrid, 29 June 2022» (2022), (7). https://www.nato.int/strategic-concept/.

[16] "72. We have taken steps to ensure our ability to effectively address the challenges posed by hybrid warfare, where a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, are employed in a highly integrated design by state and non-state actors to achieve their objectives. Responding to this challenge, we have adopted a strategy and actionable implementation plans on NATO's role in countering hybrid warfare. The primary responsibility to respond to hybrid threats or attacks rests with the targeted nation. NATO is prepared to assist an Ally at any stage of a hybrid campaign. The Alliance and Allies will be prepared to counter hybrid warfare as part of collective defence. The Council could decide to invoke Article 5 of the Washington Treaty. The Alliance is committed to effective cooperation and coordination with partners and relevant international organisations, in particular the EU, as agreed, in efforts to counter hybrid warfare". North Atlantic Treaty Organization. «Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016» (2016), North Atlantic Treaty Organization. «Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016» (2016), (par.72). https://www.nato.int/cps/en/natohq/official_texts_133169.htm

[17] Government of the Federal Republic of Germany. «White Paper on Security Policy and the Futures of the Bundeswehr» (2016): 37. https://www.bundeswehr.de/resource/blob/4800140/fe103a80d8576b2cd7a135a5a8a86dde/download-white-paper-2016-data.pdf.

[18] *Ibid*., p. 39.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

In the same vein, the Spanish National Security Strategy unequivocally states that: "Disinformation campaigns have a clear impact on national security […]"[19]. Similarly, the US National Security Strategy of October 2022, underlined that "[...] we are responding to the ever-evolving ways in which authoritarians seek to subvert the global order, notably by weaponizing information to undermine democracies and polarize societies"[20].

In light of the serious threats to the core assets of Member States and the EU itself, including the fundamental rights of their citizens, this article examines the EU's policies and measures to combat disinformation promoted by foreign States. This analysis will allow us to evaluate the effectiveness of the measures implemented thus far in addressing current issues, while also addressing significant new questions of international law that may arise in future.

A possible future consideration is whether international organisations should be permitted to use self-defence in response to a disinformation campaign, whether alone or in conjunction with other factors, if it is deemed to constitute an armed attack[21]. This is one of the conditions set out in Article 51 of the UN Charter that would allow for the use of self-defence. To begin the discussion, I would like to express my belief that the question of whether a disinformation campaign should be considered equivalent to an armed attack should depend on the damage caused. While Article 3 of UN General Assembly Resolution 3314 ("Definition of Aggression") [22] —which is considered a synonym of "armed attacks" in international law— provides examples of such actions, including invasion, occupation of territory, bombardment and blockade of coasts or ports, Article 4 states that this list is not exhaustive. This means that the Security Council could deem other actions to constitute an armed attack. It is true that there has recently been a regrettable tendency towards self-serving laxity in setting the minimum threshold for considering an action to be an armed attack[23], given the serious consequences that the determination of an act of aggression can entail. Nevertheless, bearing in mind the necessary prudence in this field, as demonstrated by the ICJ in its case

[19] Government of Spain. «National Security Strategy» (2021): 60. https://www.dsn.gob.es/sites/default/files/documents/ESN2021%20EN.pdf.

[20] United States of America. «National Security Strategy», October. 2022 (2022): 17-18.

[21] On the necessity of being in presence of an armed attack and not only in presence of an use of force to have recourse to self-defence according to Article 51 of the UN Charter, see: Olivier Corten, «Discours de guerre, guerre de discours», *Revue interdisciplinaire d'études juridiques,* 2023/1 Volume 90 (2023): 155-176. https://doi-org.ezproxy-prd.bodleian.ox.ac.uk/10.3917/riej.090.0155.

[22] UN General Assembly, Resolution 3314 (XXIX), «Definition of Aggression», A/RES/3314(XXIX), 14 December 1974.

[23] On that point, see: Corten, «Discours de guerre, guerre de discours»: 163-167.

law, I believe the threshold should be set according to the scale of the damage caused. For example, we can consider successful disinformation campaigns that aim to promote genocide, civil war or civil strife.

The opportunity to conduct this research becomes clear when we read the foreword to the third European External Action Service (EEAS) report on foreign information manipulation and interference threats (FIMI) by the EU High Representative for Foreign Affairs and Security Policy: "Our information space has become a geopolitical battleground. From the data gathered by the EEAS, last year over eighty countries and over two hundred organisations were the targets of attacks from foreign information manipulation and interference or 'FIMI'"[24]. Furthermore, High Representative Kallas argued that: "Foreign actors use FIMI to manipulate public opinion, fuel polarisation, and interfere with democratic processes within the EU and worldwide. The aim is to destabilise our societies, damage our democracies, drive wedges between us and our partners and undermine the EU's global standing"[25]. She also suggested that: "FIMI is not merely a tool for disseminating deceptive narratives. It is an integral part of military operations used by foreign states to lay the way for kinetic action on the ground"[26]. And she concluded that: "FIMI is a major security threat to the EU"[27]. As is clear from the words of High Representative Kallas, the EU is of the opinion that disinformation campaigns can be part of hybrid tactics and thus part of warfare[28].

To address these important issues concerning the present and future of our democracies[29], our article will have an introduction and three additional sections. The second will be devoted to examining the policies and measures adopted by the EU at the beginning of the disinformation threat crisis,

---

[24] European External Action Service. «The 3rd EEAS Report on Foreign Information Manipulation and Interference Threats", Foreword by High Representative/Vicepresident Kaja Kallas» (2025). https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

[25] *Ibid*.

[26] *Ibid*.

[27] *Ibid*.

[28] In this vein, see also: Björnstjern Baade, «Fake News and International Law», *European journal of international law* 29.4 (2018): 1358. ; Suárez-Serrano, Chema, «From bullets to fake news: Disinformation as a weapon of mass distraction. What solutions does international law provide?»,. *Spanish yearbook of international law*, v. 24 (2020): 140. https://www.sybil.es/sybil/article/view/149.http://www.ejil.org/article.php?article=2924&issue=146; Chema Suárez-Serrano, «From bullets to fake news: Disinformation as a weapon of mass distraction. What solutions does international law provide?»,. *Spanish yearbook of international law*, v. 24 (2020): 140. https://www.sybil.es/sybil/article/view/149.

[29] In this sense, see: Matthias Kachelmann and Wulf Reiners, «The European Union's Governance Approach to Tackling Disinformation – Protection of Democracy, Foreign Influence, and the Quest for Digital Sovereignty», *L'Europe En Formation*, November 13 (2023): 36. https://doi.org/10.3917/eufor.396.0011.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

which can be characterised as a weak response. I have called this period "the paper war". In the third section, we will look at the period in which the EU is already taking strong measures to counter FIMI operations including disinformation campaigns. I have called this period "the real war". Finally, we will draw our conclusions.

II. **The paper war**

Disinformation campaigns originating from Russia and targeting the EU and its Member States were already being detected at the beginning of 2015. At that time, the EU began to express concern about disinformation campaigns sponsored by third countries[30], even though Russia was the more active player in those years[31]. More recently, Chinese-sponsored disinformation campaigns against European States and their allies have become increasingly frequent[32], mainly since the COVID-19 pandemic[33].

However, in the early days of the online communication revolution, when awareness of the threat posed by disinformation was just beginning to emerge, no policies or actions had yet been developed specifically to combat disinformation campaigns orchestrated by third countries[34]. This is un-

[30] In this sense, see also: *Ibid*., p. 22.

[31] On the involvement of various Russian agencies in the preparation and use of disinformation campaigns to destabilise Western States, see: Ramon Loik and Victor Madeira, «European Union Strategy and Capabilities to Counter Hostile Influence Operations»: 250, in: Holger Mölder, Vladimir Sazonov, Archil Chochia, Tanel Kerikmäe (eds) «The Russian Federation in Global Knowledge Warfare. Contributions to International Relations» (Springer, Cham 2021:247–264). https://doi.org/10.1007/978-3-030-73955-3_13. For more information on the relevance of disinformation in Russian military doctrine, see: Lucas Proto, Paula Lamoso-González and Luis Bouza García, «The Great FIMI Pivot: How the EU's Fight Against Disinformation Is Being Reframed by the European External Action Service», *Media and Communication (Lisboa)*, vol. 13 (2025): 2. https://doi.org/10.17645/mac.9474.

[32] NATO Parliamentary Assembly. Preliminary Draft Report Committee on Democracy and Security (CDS) Sub-Committee on Resilience and Civil Security (CDSRCS), March 2005, p. 7. https://www.nato-pa.int/download-file?filename=/sites/default/files/2025-04/11%20CDSRCS%2025%20E%20-%20CHINESE%20DISINFORMATION%20-%20TEITELBAUM%20REPORT.pdf. In this regard, see also: Pamment, «The EU's Role in Fighting Disinformation: Taking Back the Initiative», p. 3.

[33] European External Action Service. «1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence. February 2023». https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en.

[34] Before we proceed with our explanation of the issue and the EU's reaction to FIMI operations, it should be noted that individual countries are primarily responsible for combatting disinformation from foreign States as security is their own responsibility. The EU has not yet been granted primary competence in this matter. Furthermore, it is important to emphasise that

derstandable given that the profiles of disinformation and FIMI were not yet well-defined. In fact, as Nicolas Hénin set forth, "FIMI overlaps to a considerable extent with disinformation but some nuances need to be brought: not all disinformation is FIMI, and FIMI is not only disinformation"[35]. Having already explained in the introduction what we mean by "disinformation", it is now time to define the term "FIMI". In this regard, it is useful to recall that, for the EEAS, which is a very relevant actor for the purposes of this article, as far as, according to its own words "[…] has taken a leading role in addressing this challenge […]"[36]. FIMI

> "describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory"[37].

Therefore, "FIMI" is a strategic framework that describes complex, organised and hostile campaigns, typically carried out by foreign actors, and is a relatively new concept[38]. Meanwhile, disinformation is a type of content that may be part of an FIMI campaign, but it can also exist in isolation or domestically, and it is a more traditional concept.

Moreover, according to the European Union Agency for Cybersecurity (ENISA) and the EEAS, "The concept of FIMI puts emphasis on manipula-

---

this phenomenon affects many different areas. Not only does it affect hybrid threats, but it also affects the digital single market, media regulation in the EU and its Member States. Therefore, the regulation of disinformation is based on a broad and complex EU regulatory framework that predates the recent surge in this phenomenon, as it has been already underlined (Carlos Espaliú Berdud, «Legal and Criminal Prosecution of Disinformation in Spain in the Context of the European Union», *El Profesional de la información*, vol. 31, no. 3 (2022): 4. https://doi.org/10.3145/epi.2022.may.22; Raquel Seijas, «Las soluciones europeas a la desinformación y su riesgo de impacto en los derechos fundamentales», *IDP, Revista de internet, derecho y política*, n. 31 (2020): 3. https://raco.cat/index.php/IDP/article/view/373664/467277.

[35] Nicolas Hénin, «FIMI: Towards a European Redefinition of Foreign Interference», April 2023. EU DisinfoLab: 4. https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf.

[36] European External Action Service. «Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)». Strategic Communication. 14 March 2025. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#104621.

[37] European External Action Service (EEAS), February 2023, «1st EEAS Report on Foreign Information Manipulation and Interference Threats»: 25. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en.

[38] In that sense see: Proto, Lamoso-González and Bouza García, «The Great FIMI Pivot: How the EU's Fight Against Disinformation»…, p. 3.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

tive behaviour as the main indicator of an attack instead of content and its truthfulness. From this perspective, the manipulation of the information environment is only one aspect of FIMI, although a prominent one"[39].Thus, while there are differences between "disinformation" and "FIMI", these almost disappear when referring to "disinformation campaigns orchestrated by foreign States" rather than simply "disinformation". For the purposes of this article, we will treat "FIMI" likewise, as almost interchangeable with "disinformation campaigns sponsored by foreign States".

Returning to the EU's initial fight against disinformation in general and, later, more specifically against disinformation sponsored by third countries, when the importance of this specific phenomenon was already fully understood, let us remember that the European Council invited the High Representative to develop an action plan on strategic communication, in collaboration with the Member States and EU institutions. This resulted in the creation of the East StratCom Task Force, which has been operational since September 2015 and forms part of the Information Analysis and Strategic Communications Division of the EEAS[40]. Since then, the Task Force's main goal has been to develop communication tools and information campaigns that offer a clearer explanation of EU policies in Eastern European countries. These campaigns are intended to counter the effects of Russian propaganda against the EU. Secondly, the Task Force seeks to bolster the media landscape in the region[41]. Over the years, we have witnessed the expansion of this task force's remit, which now encompasses not only the threat of disinformation from Russia, but also that from China[42]. Indeed, since 2018, the East StratCom Task Force has closely tracked the trajectory of China's overt and covert online propaganda campaigns, first attempting to shape the perception of the Chinese diaspora and then trying to discredit dissidents and the Hong Kong protest movement[43].

---

[39] European Union Agency for Cybersecurity, & European Union External Action Service. «Foreign information manipulation interference (FIMI) and cybersecurity—Threat landscape» (2022): 7.

[40] European Council. «Conclusions of the Meeting of 19 and 20 March 2015, Document EUCO 11/15 CO EUR 1 CONCL 1». Brussels, 20 March, point. 13.

[41] On the work of the East StratCom Task Force, see: Alessia D'Andrea, Giorgia Fusacchia and Arianna D'Ulizia «Policy Review: Countering Disinformation in the Digital Age — Policies and Initiatives to Safeguard Democracy in Europe» *Information Polity*, vol. 30, no. 1 (2025): 85-86. https://doi.org/10.1177/15701255251318900.

[42] On this issue, see: EUvsDisinfo, «To challenge Russia's ongoing disinformation campaigns: Eight years of EUvsDisinfo. EUvsDisinfo» (2023). https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-eight-years-of-euvsdisinfo/.

[43] EUvsDisinfo. Jacob Wallis and Albert Zhang, «The Chinese Communist Party's information operations to shape international perception of its regime in Xinjiang» (2022). https://

A few months after the East StratCom Task Force was set up, the EU Global Strategy (2016) also referred to strategic communication as a means of providing "rapid, factual rebuttals of disinformation"[44].

Furthermore, in June 2017, the European Parliament began considering the need to adopt legal instruments to address disinformation and the spread of false content[45].

Some months afterward, in January 2018, the European Commission set up a High-Level Expert Group (HLEG) to advise on policy initiatives to combat fake news and disinformation spread online, which was very important for the development of EU action in this area[46]. Its final report, published on 12 March 2018, examined best practices in light of fundamental principles and the appropriate responses derived from them, and proposes a multi-dimensional approach to this issue to the European Commission[47]. In fact, the HLEG recommended a self-regulatory approach as a first step. This approach would be based on a clearly defined multi-stakeholder engagement process framed within a binding roadmap for implementation. The aim would be to include all stakeholders in future actions, emphasise the need for self-regulation and focus on a set of short— and medium-term actions[48]. After evaluating the effectiveness and efficiency of these measures in 2019, in a second step, the Commission should reconsider the matter with a view to deciding whether to consider further measures in the future, including regulatory or co-regulatory interventions, competition instruments, or mechanisms to ensure continuous monitoring and evaluation of self-regulatory measures[49].The report also recommended a number of additional measures, such as promoting media literacy among the population,

---

euvsdisinfo.eu/the-chinese-communist-partys-information-operations-to-shape-international-perception-of-its-regime-in-xinjiang/.

[44] European External Action Service (EEAS), «*Shared vision, common action – A stronger Europe – A global strategy for the European Union's foreign and security policy*», Publications Office (2016). https://data.europa.eu/doi/10.2871/9875.

[45] European Parliament. European Parliament resolution of 15 June 2017 on online platforms and the digital single market (2016/2276(INI)).

[46] In that sense, see: Carlos Espaliú Berdud, «Legal and Criminal Prosecution of Disinformation in Spain in the Context of the European Union», *Profesional de la información* 31 (3) (2022): 4. https://doi.org/10.3145/epi.2022.may.22.

[47] Andrea Renda, «The Legal Framework to Address 'Fake News': Possible Policy Actions at the EU Level», *Policy File*, Centre for European Policy Studies (2018): 21. https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA(2018)619013_EN.pdf.

[48] See, Madeleine De Cock Buning, «A multi-dimensional approach to disinformation : report of the independent High level Group on fake news and online disinformation», Luxembourg : Publications Office of the European Union (2018): 35. https://hdl.handle.net/1814/70297.

[49] *Ibid*.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

developing tools to empower consumers and journalists in dealing with the phenomenon of disinformation, and protecting the diversity and sustainability of European media.

Moreover, the HLEG's report recommended the development of a code of principles for online platforms and social media to adopt. This code would include the need for transparency when explaining how algorithms select news items to present. With regard to monitoring the implementation of the proposed measures, the report recommended establishing a multilateral coalition of stakeholders to ensure all agreed measures are implemented, monitored and reviewed regularly[50]. However, no official control or monitoring system was envisaged. In addition, it is interesting to note the complete lack of recommendations to EU authorities regarding the adoption of binding legal rules for member States[51].

In response to these suggestions, the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy developed the Action Plan against Disinformation in March 2018, which was approved by the European Council in December of that year[52]. The plan acknowledges the necessity of political commitment and coordinated action among EU institutions, Member States, civil society, and private entities, especially online platforms[53]. This unified action should be based on four pillars: i) improving the capacity of EU institutions to detect, analyse and expose disinformation, ii) strengthening coordinated and joint responses to disinformation, iii) mobilising the private sector to tackle disinformation and iv) raising awareness and enhancing societal resilience.

Following the implementation of the 2018 action plan, the EU's Rapid Alert System was set up to facilitate the exchange of information and coor-

---

[50] *Ibid*.

[51] Claire Wardle et al., «Seis puntos claves del informe sobre desinformación del grupo de expertos de la Comisión Europea», Maldita, 12 marzo 2018. https://maldita.es/maldita/20180312/seis-puntos-claves-del-informe-sobre-desinformacion-del-grupo-de-expertos-de-la-comision-europea.

[52] European Commission and High Representative of the Union for Foreign Affairs and Security Policy. Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. «Action Plan against Disinformation». Brussels, 5 December 2018 JOIN(2018) 36 final. Regarding the conception of the plan, see: Francisco Fonseca-Morillo, «Prólogo: La Europa que protege, de la teoría a la práctica gracias al pensamiento crítico y la alfabetización digital», *Revista de estilos de aprendizaje*, v. 13, n. 26 (2020): 2. https://doi.org/10.55777/rea.v13i26.2593.

[53] On the role of online platform in the implementation of the plan, see: Paolo Cavaliere, «From Journalistic Ethics to Fact-Checking Practices: Defining the Standards of Content Governance in the Fight against Disinformation», *The Journal of Media Law*, vol. 12, no. 2 (2020): 133-165, https://doi.org/10.1080/17577632.2020.1869486.

dinate responses to disinformation campaigns between EU institutions and Member States. The system is based on open-source information and draws on the expertise of academia, fact-checkers, online platforms and international partners. Its primary aim is to combat disinformation campaigns that interfere with or undermine European democratic processes. It focuses on two categories of phenomena: (a) campaigns originating from or supported by foreign actors, and (b) campaigns seeking to influence national or European elections[54].

Similarly, in April 2018, the European Commission proposed a code of practice to encourage private organisations, particularly online platforms, to help combat disinformation[55]. This code implied self-regulatory rules which private operators were encouraged to voluntarily accept in order to help the European Commission achieve its objectives. These rules set out a wide range of commitments, including transparency in political advertising, closing false accounts and preventing disinformation providers from monetising their content. The Code of Practice was made available for signature by the main operators in this field and, by mid-2021, many of these (including Facebook, Google, Microsoft, Mozilla, TikTok and Twitter) had signed it [56].

However, we must also acknowledge that the Covid-19 pandemic was accompanied by powerful disinformation campaigns that further obscured the aforementioned situation. In a joint communication in June 2020, for example, the European Commission and the High Representative of the EU warned that some foreign actors and certain third countries —particularly Russia and China— had undertaken disinformation campaigns concerning the virus in the EU, its surroundings and on a global scale, with the aim of undermining democratic debate and exacerbating social polarisation[57]. Together with the deteriorating geopolitical and international relations landscape, this fact made it clear to European authorities that they needed to

[54] On the rapid alert system and its implementation, see: D'Andrea, Fusacchia and D'Ulizia , «Policy Review: Countering Disinformation in the Digital Age — Policies and Initiatives to Safeguard Democracy in Europe»…, pp. 82–91. See also: Proto, Lamoso-González and Bouza García, «The Great FIMI Pivot: How the EU's Fight Against Disinformation»…, p. 9.

[55] European Commission. Code of Practice on Disinformation (2018). https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

[56] European Commission. «Code of Practice on disinformation: Commission welcomes new prospective signatories and calls for strong and timely revision». Press Release 1st October 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4945.

[57] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions. «Tackling COVID-19 disinformation — Getting the facts right». Brussels 10 June 2020. JOIN(2020) 8 final. https://eur-lex.europa.eu/legal-content/IT-EN/TXT/?uri=CELEX%3A52020JC0008.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

strengthen their policies against disinformation, particularly that originating from foreign powers[58].

In this vein, an Action Plan for European Democracy was adopted in December 2020. This emphasised existing approaches to disinformation and reaffirmed the need for the EU to systematically utilise the full range of available tools to counter foreign interference and influence operations, thereby preserving and strengthening democratic life. The Action Plan also highlights the importance of further developing these tools, particularly by imposing sanctions on those responsible[59].

When it comes to assessing its effectiveness, the absence of legal commitments and robust rules in the 2018 Code of Practice was noted in the European Commission's initial evaluation report on the implementation and effectiveness of the Code of Practice on Disinformation in 2020[60]. Indeed, alongside the Commission's perception of the ineffectiveness of the 2018 Code of Practice on Disinformation, it is interesting to note that the literature on this topic also reflects widespread scepticism about the effectiveness of self-regulatory institutions in general, and press councils in particular — a scepticism that is shared by journalists themselves[61]. Consequently, many have called for stricter measures to be implemented through hard law instruments at both national and EU levels[62].

Thus, a reform process of the 2018 Code was undertaken, involving its signatories together with some new entities. A new instrument was then drafted and published on 16 June 2022 under the name "Strengthened 2022 Code of Practice on Disinformation" [63], which is still in force today.

---

[58] In that sense, see, for instance: Petros Iosifidis, Nicholas Nicoli, «European Policy Strategies in Combating Digital Disinformation», *Digital Democracy, Social Media and Disinformation*, 1st ed., vol. 1, Routledge (2021): 61. https://doi.org/10.4324/9780429318481-7.

[59] European Commission. Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions. «On the European democracy action plan». Brussels, 3 December 2020 COM(2020) 790 final: 21. EUR-Lex — 52020DC0790 — EN — EUR-Lex.

[60] European Commission. «Commission Staff Working Document. Assessment of the Code of Practice on Disinformation — Achievements and areas for further improvement, SWD(2020) 180 final», Brussels, 10 September 2020. https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement.

[61] Cavaliere, «From Journalistic Ethics to Fact-Checking Practices: Defining the Standards of Content Governance in the Fight against Disinformation»…, p. 149.

[62] Anna Kobernjuk, Agnes Kasper, «Normativity in the EU's Approach towards Disinformation», *TalTech Journal of European Studies*, vol. 11, no. 1 (2021): 186-195. https://doi.org/10.2478/bjes-2021-0011.

[63] European Commission. «The 2022 Code of Practice on Disinformation». https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

The Strengthened Code addresses the shortcomings of the previous code by setting out more robust and detailed commitments and measures based on operational lessons learned in recent years[64]. These lessons included the impact of the pandemic and Russia's use of disinformation for military purposes in its plan to invade Ukraine.

It was the use of disinformation as a weapon in Russia's war effort during its invasion of Ukraine in 2022 that finally prompted EU authorities to change their policy[65] towards a more regulatory approach. While almost all EU institutions tried to contribute to the fight against disinformation[66], they also emphasised geopolitical considerations, thereby granting a prominent role to the EEAS[67]. For instance, the Strategic Security and Defence Compass adopted by the Council of the European Union it clearly underlines that Russia threatens the European order when it comes to the security and protection of European citizens, not only through armed aggression, but also using information manipulation campaigns[68].

The conflict therefore moved from the domain of words to that of actions, which resulted in the implementation of much more stringent measures. Initial European policies in this field were indeed strongly criticised by many experts, including Pamment, who characterised the EU's policy on disinformation as follows:

> "[...] by a lack of terminological clarity, unclear and untested legal foundations, a weak evidence base, an unreliable political mandate, and a variety of instruments that have developed in an organic rather than a systematic manner. The limited successes the EU has achieved so far –in terms of the creation of instruments such as the Code of practice on Disinformation, the Action Plan Against Disinformation, the East StratCom Task Force, and the Rapid Alert System– have been hard earned" [69].

---

[64] In that direction, see: Iosifidis, Nicoli, «European Policy Strategies in Combating Digital Disinformation»…, p. 61.

[65] For more information on the EU's evolving stance on foreign intervention through disinformation, see: Loik, Madeira, «European Union Strategy and Capabilities to Counter Hostile Influence Operations»…, p. 248.

[66] In this sense, see: Kachelmann, Reiners, «The European Union's Governance Approach to Tackling Disinformation – Protection of Democracy, Foreign Influence, and the Quest for Digital Sovereignty»…, p. 27.

[67] Proto, Lamoso-González and Bouza García, «The Great FIMI Pivot: How the EU's Fight Against Disinformation»…, p. 1.

[68] Council of the European Union (2022). «A Strategic Compass for Security and Defence. For a European Union that protects its citizens, values and interests and contributes to international peace and security»: 5.

[69] Pamment, «The EU's Role in Fighting Disinformation: Taking Back the Initiative»..., p. 5. In this regard, see also: Loik, Madeira, «. European Union Strategy and Capabilities to Counter Hostile Influence Operations»…., p. 252.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

III. **The real war**

1. *On the EU's response to disinformation campaigns in a context of growing rivalry and foreign hostility*

In the previous section, we observed a change in the EU's hard law policies aimed at combatting disinformation. This was prompted by the ineffectiveness of earlier measures and the growing seriousness of the threat posed by disinformation campaigns. This threat was particularly evident during the pandemic and in recent attacks from Russia, which became especially apparent when Russia invaded Ukraine. Nevertheless, it should be noted that a similar trend can be seen among the EU's Member States and, more broadly, in Western States[70].

One manifestation of this change in EU's policies is the 2022 Strengthened Code of Practice on Disinformation. As previously mentioned, this includes improvements on the 2018 version, particularly with regard to control and oversight mechanisms. As these features are now closer to hard law, we analyse them in this section. In this regard, it should be noted that rigour and transparency were sought by establishing two specific bodies. Firstly, a Transparency Centre has been set up to provide an overview of the implementation of the Code's measures and to make the process more transparent[71]. At the same time, a Task Force comprising representatives of the signatories, the European Regulators Group for Audiovisual Media Services (ERGA), the European Digital Media Observatory (EDMO) and the EEAS has been established[72]. The Commission is chairing this group.

Furthermore, with regard to the monitoring framework, it should be noted that the new Code incorporates service-level indicators to measure its implementation in member States and the EU. It also contains a clear commitment to establishing structural indicators to measure the Code's overall impact on misinformation[73]. In this context, it was anticipated that the signatories would provide the Commission with the first baseline reports on their implementation of the Code in early 2023. Thereafter, large online

---

[70] With regard to NATO countries, see: North Atlantic Treaty Organization Parliamentary Assembly. Policy Recommendations adopted in 2025 178 SESA 25 E | 13 October 2025. Taking NATO Deterrence and Defence to the Next Level at The Hague Summit Declaration 496*, (2025): 10. https://www.nato-pa.int/download-file?filename=/sites/default/files/2025-10/2025%20-%20NATO%20PA%20POLICY%20RECOMMENDATIONS.pdf

[71] European Commission. «The 2022 Code of Practice on Disinformation»…, Commitments 34-36.

[72] *Ibid*., Commitment 37.

[73] *Ibid*., Commitments 40-42.

platforms, as defined in the Digital Services Act (DSA)[74], were to report every six months, while other signatories were to report annually.

As we can observe, the Strengthened Code forms part of a broader regulatory framework, alongside legislation on transparency and targeting of political advertising and the DSA. Regarding the former, the European Parliament and the Council recently adopted a new regulation in 2024 which aims to counter information manipulation and foreign interference[75]. For example, to avoid external influences, the provision of advertising services to sponsors from third countries is prohibited during the three months preceding an EU election or referendum[76]. It is interesting to note that Article 25 provides for penalties for sponsors or political advertising service providers who breach their main obligations, amounting to up to 6% of the sponsor's or political advertising service provider's total annual revenue or budget, or 6% of their worldwide turnover in the preceding financial year[77]. The Regulation has been fully operational since October 2025, as set out in Article 30, and therefore none of the fines mentioned have been imposed.

On the other hand, on 13 February 2025, the Commission endorsed the official integration of the 2022 Strengthen Code of Practice on Disinformation into the framework of the DSA and its conversion into a Code of Conduct[78]. After integration, compliance with the Code will be considered an appropriate risk mitigation measure for signatories designated as very large online platforms (VLOPs) and very large online search engines (VLOSEs) under the DSA. The Code will thus become an important and significant reference point for determining compliance with the DSA. Compliance with the obligations under the Code will also be part of the annual independent review to which these platforms are subject under the DSA.

Regarding the DSA, it should be noted that it imposes significant obligations on large online platforms and search engines. As announced earlier, the Regulation classifies platforms or search engines with more than 45

---

[74] 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) (Text with EEA relevance), PE/30/2022/REV/1, *OJ L 277,* 27 October 2022, Article 33.

[75] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (Text with EEA relevance), PE/90/2023/REV/1 *OJ L,* 2024/900*,* 20 March 2024. *http://data.europa.eu/eli/reg/2024/900/oj*

[76] *Ibid*., Article 5.

[77] *Ibid*., Article 25.

[78] Commission of the European Union. «Commission endorses the integration of the voluntary Code of Practice on Disinformation into the Digital Services Act». Press Release of 13 February 2025. https://digital-strategy.ec.europa.eu/en/news/commission-endorses-integration-voluntary-code-practice-disinformation-digital-services-act.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

million users per month in the EU as VLOPs or VLOSEs[79]. These companies must, among other things, report criminal offences, have user-friendly terms and conditions, be transparent about advertising, recommendation systems or content moderation decisions, and demonstrate a proactive profile in looking for systemic risks associated with their services in terms of illegal content, public safety, fundamental rights, etc[80]. Importantly, in case of non-compliance with the key obligations included in its articles, fines of up to 6% of the annual worldwide turnover or temporary suspension of the service can be imposed[81]. In view of the possible adoption of decisions under Articles 73 and 74 of the Regulation regarding the conduct of very large online platforms or search engines suspected by the Commission of infringing any of the Regulation's provisions, it should be noted that, as of November 2025, the Commission had opened a total of 10 infringement procedures, but had not yet imposed any penalties[82]. Nevertheless, in four cases, the Commission has preliminarily found that four online platforms have violated the obligations contained in the DSA, which is a preliminary step before fines are imposed. First, on 15 May 2025, the Commission announced that it had informed the social media and online video platform TikTok of its preliminary view that it does not fulfil the DSA's obligation to publish an advertisement repository[83]. Second, on 18 June 2025, the Commission found preliminarily that AliExpress, the global online retail marketplace owned by the Alibaba Group, was in breach of its obligation to assess and mitigate risks related to the dissemination of illegal products under the DSA[84]. Third, on 28th July 2025, the Commission found Temu in breach of the obligation under the DSA to properly assess the risks of illegal products

---

[79] 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) (Text with EEA relevance), PE/30/2022/REV/1, *OJ L 277,* 27 October 2022, Article 33.

[80] *Ibid.,* Articles 34-43.

[81] *Ibid.,* Articles 52, 73-74 and 76. On the more robust measures imposed on VLOP and VLOSE under the DSA, see, for example: Kachelmann, Reiners, «The European Union's Governance Approach to Tackling Disinformation – Protection of Democracy, Foreign Influence, and the Quest for Digital Sovereignty»…, p. 30.

[82] In this regard, see: European Commission. Supervision of the designated very large online platforms and search engines under DSA, https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.

[83] European Commission. Press Release of 15th May 2025. «Commission preliminarily finds TikTok's ad repository in breach of the Digital Services Act». https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1223.

[84] European Commission. Press Release of 18th June 2025. «Commission accepts commitments offered by AliExpress under the Digital Services Act and takes further action on illegal products». https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1551.

being disseminated on its marketplace[85]. Finally, on 24 October 2025, the Commission preliminarily found both TikTok and Meta were in breach of their obligation to grant researchers adequate access to public data under the DSA and also that Meta was in breach of its obligations to provide users simple mechanisms to notify illegal content, as well as to allow them to effectively challenge content moderation decisions[86].

Returning to the activation of more specific measures and policies established by the EU against FIMI and foreign actors behind disinformation campaigns, the adoption of the 2022 Strategic Security and Defence Compass by the Council of the European Union can be considered a turning point. It paved the way for stronger policies and measures within the scope of the Common Foreign and Security Policy (CFSP). As set out in the text, the Council announced the creation of an EU Hybrid Toolbox to detect and respond to a broad range of hybrid threats. Among these possible measures was the development of a specific "[…] EU toolbox to address and counter foreign information manipulation and interference […]"[87]. According to the EEAS, the Toolbox takes a whole-of-society approach based on four pillars: situational awareness, building resilience, disruption and regulation, and external action[88].

Another step in this direction was taken on 7 February 2023 when the High Representative and Vice-President of the European Union announced the creation of an Information Sharing and Analysis Centre (ISAC) at the EEAS conference on foreign manipulation and interference in the information sphere. The centre's mission is to facilitate the sharing of information, experience, expertise, and analysis between all stakeholders regarding the causes, incidents, and threats of foreign manipulation and interference in the information sphere[89].

---

[85] European Commission. Press Release of 28th July 2025. «Commission preliminarily finds Temu in breach of the Digital Services Act in relation to illegal products on its platform». https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1913.

[86] European Commission. Press Release of 24 October 2025. «Commission preliminarily finds TikTok and Meta in breach of their transparency obligations under the Digital Services Act». https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503.

[87] Council of the European Union (2022). «A Strategic Compass for Security and Defence. For a European Union that protects its citizens, values and interests and contributes to international peace and security»: 22.

[88] European External Action Service. «Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)». «EEAS responses to Foreign Information Manipulation and Interference (FIMI)». Strategic Communication. 14 March 2025.

[89] Foreign Information Manipulation and Interference (FIMI) – Information Sharing and Analysis Centre (ISAC). https://fimi-isac.org/index.html. On the creation of this new centre against FIMI, see, for example: Proto, Lamoso-González and Bouza García, «The Great FIMI Pivot: How the EU's Fight Against Disinformation»…, p. 9.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

However, of all the policies and measures adopted by the EU against disinformation campaigns orchestrated by foreign countries, the sanctions regime is the most notable. It was established by the Council of the EU through Decision (CFSP) 2024/2643 on 8 October 2024[90]. This was in response to the growing number of hybrid activities targeting the Union and its Member States, which had already been condemned by the EU and its institutions in previous months[91], as mentioned above. In accordance with that instrument, restrictive measures should be imposed on individuals, organisations or bodies responsible for, involved in the implementation of, or providing support for the aforementioned actions or policies of the Government of the Russian Federation[92]. These sanctions should consist of a prohibition on the entry into and transit through the territory of Member States of the individuals listed in the subsequent instruments, and the freezing of funds and economic resources belonging to those individuals or legal persons listed in those instruments[93]. Indeed, within the framework created by Decision (CFSP) 2024/2643, additional instruments have been introduced to develop and specify the initial provisions, as well as to establish the names of the individuals and institutions subject to sanctions[94]. On 20 May 2025, the EU expanded the sanctions regime to include assets related to Russia's destabilising activities, such as vessels, aircraft, real estate, and physical elements of digital and communications networks. It also covered transactions by credit and financial institutions, as well as entities providing cryptocurrency services. More people and institutions were also added to the list of those previously sanctioned[95]. As a result of this sanctions regime, 47 individuals and 15 entities are currently sanctioned[96]. These in-

[90] Council Decision (CFSP) 2024/2643 of 8 October 2024 concerning restrictive measures in view of Russia's destabilising activities, ST/8742/2024/INIT, *OJ L,* 2024/2643, 9 October 2024. *ELI: http://data.europa.eu/eli/dec/2024/2643/oj*.

[91] *Ibid*., recitals 10–15.

[92] *Ibid*., recital 16.

[93] *Ibid*., Articles 1 and 2.

[94] Council Implementing Regulation (EU) 2024/3188 of 16 December 2024 implementing Regulation (EU) 2024/2642 concerning restrictive measures in view of Russia's destabilizing activities, ST/15799/2024/INIT, *OJ L,* 2024/3188, 16 December 2024. *ELI: http://data.europa.eu/eli/reg_impl/2024/3188/oj*

[95] See: Council Decision (CFSP) 2025/963 of 20 May 2025 amending Decision (CFSP) 2024/2643 concerning restrictive measures in view of Russia's destabilising activities, ST/8424/2025/INIT, *OJ L,* 2025/963, 20 May 2025, ELI: http://data.europa.eu/eli/dec/2025/963/oj. And Council Decision (CFSP) 2025/966 of 20 May 2025 amending Decision (CFSP) 2024/2643 concerning restrictive measures in view of Russia's destabilising activities, ST/5953/2025/INIT, *OJ L,* 2025/966, 20 May 2025, ELI: http://data.europa.eu/eli/dec/2025/966/oj.

[96] Council of the European Union. «EU sanctions against Russia». https://www.consilium.europa.eu/en/policies/sanctions-against-russia/#hybrid.

clude individuals disseminating pro-Russian propaganda in Ukraine, individuals involved in activities aimed at undermining the democratic political processes in Estonia and Germany, and individuals involved in the so-called 'Doppelgänger' campaign[97] — the Russian disinformation campaign aimed at undermining support for Ukraine following the invasion.

Furthermore, since Russia's invasion of Ukraine in 2022, the Council of the European Union[98] has suspended the broadcasting licences of several Kremlin-backed outlets that disseminate disinformation, as part of the measures included in the FIMI "toolbox". The Russian government had exploited these outlets to manipulate information and spread misinformation about its military aggression against Ukraine. This includes propaganda aimed at destabilising countries bordering Russia and EU Member States. The broadcasting ban currently applies to 27 media outlets[99].

In this regard, it is important to note that the Court of Justice of the European Union has confirmed the legal basis for the sanctions imposed by the Council. Indeed, in its judgment of 27 July 2022, the General Court dismissed Russia Today France's application to annul the Council's acts. Russia Today France, one of the suspended media outlets, sought to annul the contested acts on the grounds that its rights to defence, freedom of expression and information, and freedom to conduct business had been infringed. The applicant also alleged an infringement of the principle of non-discrimination. Furthermore, it questioned the Council's competence to adopt the contested measures. However, the General Court dismissed RT France's application against the Council of the EU's restrictive measures, which prohibited the broadcasting of RT France's content within the EU's territory. The Court confirmed that the Council had acted within its powers under the CFSP and that the measures responded to an urgent situation involving a serious threat to public order and security within the EU. The Court considered the restrictions on fundamental rights, including the right to defence, freedom of expression and freedom to conduct business, to be valid as they were provided for by law, proportionate and pursued legitimate objectives, such as protecting democratic debate from disinformation campaigns promoted by State-controlled Russian media outlets. The Court also rejected the existence

---

[97] *Ibid*.

[98] See: Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, *OJ L* 65, 2 March 2022, pp. 1-4 and 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, *OJ* L 65, 2 March 2022, pp. 5-7.

[99] Council of the European Union. «EU sanctions against Russia. Bans on media outlets». https://www.consilium.europa.eu/en/policies/sanctions-against-russia/#hybrid.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

of discrimination on the grounds of nationality, since the difference in treatment was based on the media being controlled by a third country that was acting as an aggressor, and not on the nationality of its owners[100].

2. *On the possible responses of the EU to disinformation campaigns in a war context*

So far, we have examined how the EU has gradually strengthened its measures and policies against disinformation campaigns in recent years. And in the previous section, we analysed the EU's reactions to the use of disinformation to destabilise it or its Member States in a context of open rivalry or hostility with Russia, which is what has actually happened since the invasion of Ukraine in 2022. A similar situation arose when evidence of Russian interference in the 2016 United States elections through disinformation campaigns and cyberattacks was presented in a report by the US Senate Select Committee on Intelligence[101]. In response to this interference, the Obama administration took action against Russia, for example by imposing sanctions on Russian individuals and companies, expelling Russian government personnel, and closing certain Russian diplomatic properties on US territory[102].

In the context of international law, the responses of both the US and the EU could be considered countermeasures, for they violate previous obligations, but do not incur international responsibility, as they have been adopted in response to previous violations by Russia. In this regard, it is worth noting that the possibility of international organisations having recourse to countermeasures is currently widely accepted, as acknowledged by the International Law Commission (ILC) in its 2011 Draft Articles on the Responsibility of International Organisations. The Commission also set out the circumstances in which international organisations can resort to countermeasures, essentially mirroring the rights of States[103].

---

[100] See: General Court. Judgment of the General Court (Grand Chamber), 27 July 2022, *RT France, v Council of the European Union,* Case Case T-125/22. ECLI:EU:T:2022:483. See also: Court of Justice of the European Union. Press Release No 132/22 Luxembourg, 27 July 2022. «The Grand Chamber of the General Court dismisses RT France's application for annulment of acts of the Council, adopted following the outbreak of the war in Ukraine, temporarily prohibiting that organisation from broadcasting content». https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-07/cp220132en.pdf.

[101] United States of America Senate. U.S. Senate Select Committee on Intelligence, «Russian active measure campaigns and interference in the 2016 U.S. Election», 2020.

[102] *Ibid.,* vol. III, pp. 181, 194-195.

[103] See articles 22 and 51-57 of the «International Law Commission Draft articles on the responsibility of international organizations, with commentaries, 2011». Report of the Com-

However, in view of Russia's growing animosity, we must now take a step forward and place ourselves in a context of a possible future war. In that regard, we must ask ourselves how the EU would react to disinformation campaigns orchestrated by foreign powers that amount to actual armed attacks, either alone or in combination with other elements[104]. As an alternative, we could consider whether the EU has the right to self-defence in the event of a disinformation campaign that could constitute an armed attack, either alone or in conjunction with other aggressive elements, as required in Article 51 of the United Nations Charter. In this regard, we should start by noting that, from the perspective of international law, the possibility of international organisations resorting to self-defence is not currently considered problematic in principle, even though Article 51 of the United Nations Charter only refers to States in this context. Indeed, as was the case with countermeasures, the 2011 ILC Draft Articles on the Responsibility of International Organisations recognise that self-defence can preclude wrongfulness in the case of international organisations[105]. Similarly, it is noticeable that the current state of international law has made clear progress in relation to other aspects of self-defence compared to the situation when the United Nations Charter was adopted. Consider, for example, the possibility of resorting to self-defence in the event of a large-scale attack carried out by a non-State actor, such as a terrorist organisation. Indeed, it seems that a precedent is emerging in favour of States exercising self-defence in such circumstances, given the recent practice to major attacks[106].

---

mission to the General Assembly on the work of its sixty-third session. *Yearbook of the International Law Commission, 2011, vol. II, Part Two*. Document United Nations A/CN.4/SER.A/2011/Add.1 (Part 2), pp. 71-72 and 92-96.

[104] For example, to support our statement, we can point out that a document published in 2022 by a group of civil society experts established by the Spanish Government's Department of National Security states that: " Una campaña organizada de desinformación puede constituir, dependiendo de su alcance, naturaleza y efectos, una violación de los principios de soberanía o de no intervención, o una amenaza, un uso de la fuerza, un ataque armado o una agresión contraria al Derecho Internacional". (An organised disinformation campaign may, depending on its scope, nature and effects, constitute a violation of the principles of sovereignty or non-intervention, or a threat, use of force, armed attack or aggression contrary to international law) (translation is ours). See: Gobierno de España. Presidencia del Gobierno. « Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional. Propuestas de la sociedad civil »…, p. 79.

[105] See, «International Law Commission Draft articles on the responsibility of international organizations, with commentaries, 2011»…, Article 21, p. 71.

[106] In this sense, see: Carlos Espaliú Berdud, «The EU Response to the Paris Terrorist Attacks and the Reshaping of the Right of Self-Defence in International Law», *Spanish Yearbook of International Law* 20 (December) (2016): 206-207. https://www.sybil.es/sybil/article/view/1391.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

On the other hand, a very important precedent regarding the possibility of the EU resorting to self-defence in the context of international responsibility is the military and financial aid that the international organisation has been providing to Ukraine since the Russian invasion. In addition to imposing sanctions, the EU has used various mechanisms to provide Ukraine with weapons, training and financial aid so that it can defend itself against Russian aggression. However, probably to avoid being considered a direct participant in the conflict, the EU has never stated that all this aid was provided as part of Ukraine's exercise of collective self-defence[107]. Indeed, in terms of providing weapons, the Council decided in its Council Decision (CFSP) 2022/338 of 28 February 2022 to supply Ukraine with military equipment and platforms designed to deliver lethal force[108]. Since then, it has adopted several decisions with the same aim[109]. Moreover, by its Decision (CFSP) 2022/1968 of 17 October 2022, the Council set up an Euro-

[107] In that sense, see also: Marko Svicevic, «European Union Military Missions and the War in Ukraine: Moving beyond the Jus Ad Bellum Framework», *Polish Review of International and European Law (Online)*, vol. 13, no. 1, (2024): 108-109. https://doi.org/10.21697/2024.13.1.04.

[108] Council Decision (CFSP) 2022/338 of 28 February 2022 on an assistance measure under the European Peace Facility for the supply to the Ukrainian Armed Forces of military equipment, and platforms, designed to deliver lethal force, *OJ* L 60, 28 February 2022, pp. 1-4. For a study of the military aid to Ukraine by the EU from the point of view of arm control, see: Tomas Hamilton, «Defending Ukraine with EU Weapons: Arms Control Law in Times of Crisis», *European Law Open* 1, no. 3 (2022): 635-659. https://doi.org/10.1017/elo.2022.35.

[109] Council Decision (CFSP) 2022/471 of 23 March 2022 amending Decision (CFSP) 2022/338 on an assistance measure under the European Peace Facility for the supply to the Ukrainian Armed Forces of military equipment, and platforms, designed to deliver lethal force (*OJ* L 96, 24 March 2022, p. 43); Council Decision (CFSP) 2022/636 of 13 April 2022 amending Decision (CFSP) 2022/338 on an assistance measure under the European Peace Facility for the supply to the Ukrainian Armed Forces of military equipment, and platforms, designed to deliver lethal force (*OJ* L 117, 19 April 2022, p. 34); Council of the European Union. Council Decision (CFSP) 2022/809 of 23 May 2022 amending Decision (CFSP) 2022/338 on an assistance measure under the European Peace Facility for the supply to the Ukrainian Armed Forces of military equipment, and platforms, designed to deliver lethal force (OJ L 145, 24 May 2022, p. 40); Council Decision (CFSP) 2022/1285 of 21 July 2022 amending Decision (CFSP) 2022/338 on an assistance measure under the European Peace Facility for the supply to the Ukrainian Armed Forces of military equipment, and platforms, designed to deliver lethal force (*OJ* L 195, 22 July 2022, p. 93); Council Decision (CFSP) 2022/1971 of 17 October 2022 amending Decision (CFSP) 2022/338 on an assistance measure under the European Peace Facility for the supply to the Ukrainian Armed Forces of military equipment, and platforms, designed to deliver lethal forcé, *OJ* L 270, 18 October 2022, pp. 95–96; Council Decision (CFSP) 2022/2245 of 14 November 2022 on an assistance measure under the European Peace Facility to support the Ukrainian Armed Forces trained by the European Union Military Assistance Mission in support of Ukraine with military equipment, and platforms, designed to deliver lethal force, *OJ* L 294, 15 November 2022, pp. 25–28; Council Decision (CFSP) 2023/927 of 5 May 2023 on an assistance measure under the

pean Union Military Assistance Mission in support of Ukraine (EUMAM Ukraine)[110]. The mission, which was officially established on 17 October 2022, aimed to enhance the military capabilities of the Ukrainian Armed Forces, enabling them to defend Ukraine's territorial integrity and sovereignty within its internationally recognised borders and protect the civilian population. EUMAM Ukraine has a non-executive mandate to provide individual, collective, and specialised training to members of the Ukrainian Armed Forces in multiple locations within EU member States. And by its Decision (CFSP) 2024/2876 of 8 November 2024, the Council extended the mission until 15 November 2026[111].

Could the assistance provided by the EU be considered equivalent to the use of force, as Russia might interpret it? To our purposes, the criteria provided by the International Court of Justice in the 1986 *Nicaragua* case would be useful. On that occasion, the Court was asked to determine whether the US's actions in providing assistance to the *contras* should be considered a use of force, despite this potentially being considered legitimate. The Court said that:

> "In the view of the Court, while the arming and training of the *contras* can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of al1 the assistance given by the United States Government. In particular, the Court considers that the mere supply of funds to the *contras*, while undoubtedly an act of intervention in the interna1 affairs of Nicaragua, as will be explained below, does not in itself amount to a use of force" [112].

Therefore, even though the case in question was a non-international conflict, the criteria established by the Court can be applied to the case of EU assistance to Ukraine, considering that these actions could constitute an use of force[113]. However, the legitimacy of the EU's probable use of force

---

European Peace Facility to support the Ukrainian Armed Forces through the provision of ammunition, *OJ* L 123, 8.5.2023, pp. 27–31.

[110] Council Decision (CFSP) 2022/1968 of 17 October 2022 on a European Union Military Assistance Mission in support of Ukraine (EUMAM Ukraine), *OJ* L 270, 18.10.2022, pp. 85-91.

[111] Council Decision (CFSP) 2024/2876 of 8 November 2024 amending Decision (CFSP) 2022/1968 on a European Union Military Assistance Mission in support of Ukraine (EUMAM Ukraine), *OJ* L, 2024/2876, 11 November 2024.

[112] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986*, pp. 118-119, paragraph 228.

[113] In that line, see also: Aurora Rasi, «Providing Weapons to Ukraine: The First Exercise of Collective Self-Defence by the European Union?», *European papers (Online. periodico)* 9.1 (2024): 421. On that point, see also: Araceli Mangas Martín, «Guerra en Ucrania: perspectiva jurídico-internacional», *Actualidad Jurídica Uría Menéndez*, 60

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

depends on whether it is justified by Ukraine's request for assistance in exercising its right to self-defence, as was also implied in the Court's judgment in 1986[114].

Another closely related, yet distinct, question is whether the EU could be held internationally responsible for the actions of the Ukrainian armed forces during the war. In this case, we believe that the criteria set out in Article 7 of the ILC's Draft Articles on the International Responsibility of International Organisations should apply. According to this provision, the conduct of an organ of an international organisation that is placed at the disposal of another international organisation (or, in this case, a State) may be considered an act of that State if it exercises effective control over the act in question. If the EU's international responsibility for possible unlawful acts committed by the Ukrainian army were to be clarified, the provisions of Article 15 of the same draft would also have to be applied. Let us recall that the text states the following:

> "Article 15. Direction and control exercised over the commission of an internationally wrongful act an international organization which directs and controls a State or another international organization in the commission of an internationally wrongful act by the State or the latter organization is internationally responsible for that act if: (a) the former organization does so with knowledge of the circumstances of the internationally wrongful act; and (b) the act would be internationally wrongful if committed by that organization".

Another question is whether the EU's actions, such as supplying weapons and training Ukrainian troops, could constitute an armed attack in themselves[115].While this analysis is not strictly necessary in this instance, we should consider the damage caused and its impact on the fundamental interests of the victim, whether they are a State or an international organisation, in order to distinguish between the simple use of force and an armed

(2022): 17. https://www.uria.com/documentos/publicaciones/8189/documento/ajum60art.pdf?id=13167&forceDownload=true.

[114] In that sense, for example: Michael Schmitt, «Providing arms and materiel to Ukraine: neutrality, Co-belligerency, and the use of force», *Article of war,* Lieber Institute, West Point, 7 March 2022 (2022). https://lieber.westpoint.edu/ukraine-neutrality-co-belligerency-use-of-force/. Araceli Mangas Martín also considers the legitimacy of EU assistance to Ukraine in the context of Ukraine's right to self-defence, see: Mangas Martín, «Guerra en Ucrania: perspectiva jurídico-internacional»…, p. 17.

[115] In this sense, it is also useful to recall that, in the *Nicaragua* case of 1986, the Court did not qualify the support, training and financing of the Contras as equivalent to an armed attack that could lead to Nicaragua taking action in self-defence. In that sense, see: Corten «Discours de guerre, guerre de discours»…, p. 162.

attack, as mentioned in the introduction. Disinformation campaigns may cause such significant damage in future that they could be considered equivalent to an armed attack in the context of Article 51 of the United Nations Charter[116].

Now that we have established that the EU could invoke self-defence in response to disinformation campaigns, either alone[117] or in conjunction with other kinetic or military elements if the violation amounts to an armed attack, we should examine the circumstances in which this could be invoked in more detail.

We have just witnessed an instance in which the EU has likely exercised collective self-defence by providing assistance to a State under attack. However, when it comes to resorting to self-defence in the face of disinformation campaigns sponsored by third States —when considered in themselves or alongside other factors as an armed attack— the question arises: What kind of measures could the EU take in such a case? What legal form could the invocation of the EU's right to exercise self-defence take?

In terms of the measures that the EU could take, it should first be noted that the Union itself is unable to use military force to defend the territory of its Member States. According to Article 4(2) TEU, the EU must respect the "essential State functions" of Member States, including "ensuring territorial integrity, maintaining law and order, and safeguarding national security". Therefore, national security remains the sole responsibility of each Member State[118], and

---

[116] Indeed, as Olivier Corten put it, with the concept of hybrid wars: "[…] manifestement, les seuils qui constituent l'essence du jus contra bellum sont mis sous pression […]". See: *Ibid*., p. 167.

[117] In the document published in 2022 by a group of civil society experts created by the Department of National Security of the Government of Spain, it is put forward that: "La acción contra las campañas de desinformación podrá implicar el ejercicio del derecho a la legítima defensa individual y colectiva en los términos y condiciones prescritos en el art. 51 de la Carta de Naciones Unidas y conforme a los acuerdos suscritos en materia de asistencia mutua en el Tratado de la Unión Europea y en el marco de la Organización del Tratado del Atlántico Norte". (Action against disinformation campaigns may involve the exercise of the right to individual and collective self-defence under the terms and conditions set out in Article 51 of the United Nations Charter and in accordance with the agreements on mutual assistance signed in the Treaty on European Union and within the framework of the North Atlantic Treaty Organisation) (the translation is ours). See: Gobierno de España. Presidencia del Gobierno. «Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional. Propuestas de la sociedad civil»…, pp. 78-79.

[118] In that sense, see: Marcus Klamert, «Article 4 TEU», in Manuel Kellerbauer, Marcus Klamert, and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (New York, 2019; online edn, Oxford Academic): 45. https://doi.org/10.1093/oso/9780198759393.003.7.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

common defence is not yet an EU competence[119]. As Thomas Ramopoulos put it: "Common defence would require a qualitatively different level of integration going beyond what is currently provided in the text of the Treaties. Such a level of deeper integration could for example entail integrated armed forces of the Union"[120]. Should Member States decide to adopt a common defence policy within the EU, this would need to be implemented via the standard Treaty reform process outlined in Articles 48(2)-(5) TEU, since amending Article 4(2) TEU is not feasible through the simplified procedure[121]. In summary, if the EU were to be attacked, it could resort to measures implying the use of force, though not amounting to an armed attack[122].

Secondly, when analysing the legal form that the invocation of the EU's right to self-defence could take, it should be noted that this event has not been anticipated. This means that there is no specific procedure for the EU to follow in order to declare its intention to invoke self-defence. Conversely, it is difficult to envisage a disinformation campaign orchestrated by foreign powers that would exclusively target the EU and constitute a genuine armed attack. If such a campaign were to occur, it would likely impact the interests of the EU and its Member States simultaneously. In this case, the Member States could invoke the procedures set out in Article 42(7) of the TEU and, of course, those of Article 5 of the NATO Treaty if they aro also part of this other organisation[123]. Article 42 (7) TEU establishes a clause of mutual assistance, obliging all Member States to defend any Member State that is subject to aggression. Therefore, in my opinion, if there is no provision in the founding treaties for the Union itself to invoke self-defence, it could take measures involving the use of force as part of a Common Security and Defence Policy (CSDP) military mission, in accordance with Articles 42(1) and 43(1) of the TEU[124]. This would be analogous to

---

[119] See: Thomas Ramopoulos, «Article 42 TEU», in Manuel Kellerbauer, Marcus Klamert, and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (New York, 2019; online edn, Oxford Academic), paragraph 14. https://doi.org/10.1093/oso/9780198759393.003.53.

[120] *Ibid*., paragraph 15.

[121] In that sense see: *Ibid*., paragraph 16.

[122] Another question is whether the EU could resort to non-military actions that would be equivalent to an armed attack due to the damage they could cause, and thus exercise its legitimate right to self-defence against such actions, such as large-scale disinformation campaigns. While the possibility remains open, I understand that it would still be a truly far-fetched case, given how difficult it is to imagine the EU carrying out a disinformation campaign against a foreign state that has previously used that weapon against it.

[123] If a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster, it can also invoke the solidarity clause included in Article 222 of the Treaty on the Functioning of the European Union.

[124] Regarding the possibility to use the force in military operations of the EU, Sven Biscop and Jo Coelmont set forth that: "The Treaty wording makes clear that this certainly in-

the Military Assistance Mission in Support of Ukraine (EUMAM Ukraine), established by Council Decision (CFSP) 2022/1968 on 17 October 2022. According to Article 42(4) TEU, such a decision would require unanimous approval by the Council of the EU. In that regard, Vladimir Kmec is right to point out that: "The EU has never used its CSDP to contain an open conflict or to act urgently to stop violence" [125]. However, given the return of insecurity that humanity is experiencing, particularly in Europe with the aggression that Russia has already demonstrated, it cannot be denied that in the future these operations will demonstrate more muscle than they have so far[126].

IV. **Conclusion**

Gradually, States and international organisations around the world have been affected by disinformation campaigns. These perverse information disorders seriously affect the fundamental rights of citizens, while at the same time potentially damaging important public interests. Disinformation campaigns sponsored by foreign States, which are being used as elements of warfare, are particularly dangerous. In this paper, we have focused on the EU's (Saint George) fight against this new dragon.

The EU has been fighting this modern plague of disinformation for a decade, particularly that promoted by third countries, with various actors, policies, media and actions, as this dragon has many heads and can only be defeated through a multidimensional effort involving public and private actors, as well as the population.

---

cludes operations at the high end of the spectrum of violence, i.e. combat operations". See: Sven Biscop and Jo Coelmont, «A Strategy for CSDP Europe's Ambitions as a Global Security Provider.» Egmont Institute (2010): 22. https://www.egmontinstitute.be/a-strategy-for-csdp-europes-ambitions-as-a-global-security-provider/

[125] Vladimir Kmec, «CSDP Machinery and Peacebuilding», *EU Missions and Peacebuilding*, 1st ed., vol. 1, Routledge (2022): 56. In that line, see also: Katarina Engberg, *The EU and Military Operations : A Comparative Analysis*. 1st ed., Routledge (2014): 181-185.

[126] According to Oleksandr Danyluk: "In parallel with the continuation of the military intervention in Ukraine, Russia has intensified its non-military aggression in western countries, using the entire spectrum of covert actions: from supporting political proxies and propaganda, to the formation of paramilitary organisations and conducting sabotage actions against critical infrastructure" (Oleksandr V. Danylyuk, «How to Resist Russia's Covert War Against the West», *International Center for Defence and Security*, Commentary, 26 June 2025 (2925). https://icds.ee/en/how-to-resist-russias-covert-war-against-the-west/) and also: "To a large extent, what Russia is using against the west today, it tried against Ukraine before the start of covert military aggression in Crimea and the Donbas in 2014, and the full-scale invasion in 2022. The Ukrainian experience should, therefore, be carefully studied" (*ibid.)*.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

However, in this fight, we have identified two stages, simply to provide greater clarity to our presentation and to highlight the evolution that has taken place as the phenomenon has become better understood and its dimensions and dangers have grown.

In the first stage, which began back in 2015 when the EU gradually became aware of this problem, soft policies and measures were implemented, promoting a self-regulatory approach by private actors involved in disinformation in general, in line with the trends of the time and the recommendations of the high-level expert group on disinformation that appeared in 2018. We have called this first stage the "paper war". As a result of these soft policies, the EU Code of Practice on Disinformation was drawn up in 2018, which essentially left the leading role in this area to the major online platforms, without establishing strict control measures or possible sanctions for non-compliance with the obligations contained in the Code.

However, given the ineffectiveness of these initial soft policies and measures, and in light of the growing awareness of the danger posed by disinformation campaigns sponsored by foreign powers, as amply demonstrated by the COVID pandemic and the invasion of Ukraine, the EU began to adopt tougher and more severe policies and measures. We have called this second phase the "real war".

An example of measures in this new era is the reform of the 2018 Code of Practice on Disinformation, which was renamed the "Strengthened 2022 Code of Practice on Disinformation". The new reformed code includes stricter control and sanctioning mechanisms, with the involvement of EU bodies and a greater role for the European Commission. Of particular note is the relationship between the new code and hard law instruments such as the Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and the Regulation (EU) 2024/900 of 13 March 2024 on the transparency and targeting of political advertising. The interrelation with these hard law instruments now makes it possible to impose heavy fines on large online platforms that have not complied with their legal obligations under this regulatory framework. For the time being, although numerous sanctioning proceedings have already been initiated, no fines have been imposed.

Alongside this, it is worth highlighting a series of more specific measures and policies established by the EU against FIMI and foreign actors behind disinformation campaigns, following the adoption of the Strategic Security and Defence Compass in 2022 by the Council of the European Union. This compass paved the way for stronger policies and measures in the field of the CFSP. As set out in the text, the Council announced the creation of a variety of EU hybrid tools designed to detect and respond to different types of hybrid threat. For instance, a specific "toolbox" was to be set up for FIMI.

The sanctions regime established by the Council of the EU through Decision (CFSP) 2024/2643 on 8 October 2024 is the most relevant of these new policies and measures. In accordance with this instrument, restrictive measures should be imposed on individuals, organisations, or bodies responsible for, involved in implementing, or providing support for the actions or policies of the Government of the Russian Federation in this context. These sanctions consist of a prohibition on entering and transiting through the territory of Member States, as well as the freezing of funds and economic resources belonging to individuals and legal persons found responsible. To date, 47 individuals and 15 entities have been sanctioned under this framework.

Moreover, since the invasion of Ukraine, the Council of the European Union has suspended the broadcasting licenses of 27 Kremlin-backed media outlets that disseminate disinformation, as part of the measures included in the FIMI "toolbox".

By projecting this set of measures that the EU has been adopting against Russian individuals and entities under the international responsibility regime of public international law, we can consider them as countermeasures, insofar as they respond to previous unlawful acts.

In addition, to gain a comprehensive understanding of the measures that the EU can take against States behind disinformation campaigns, we asked ourselves whether the international organisation could use force in response. Starting from the premise that a disinformation campaign can cause significant damage to its target, we concluded that it could be considered equivalent to the use of force, or even armed attacks if the damage were extremely serious. Therefore, we concluded that the EU could use force through CSDP missions in response to such campaigns. However, since the EU has no competence in the area of Member State territorial defence, we believe it could not invoke self-defence in response to a large-scale disinformation campaign affecting it. While such a situation is not easily foreseeable, it is more likely that disinformation campaigns will be associated with armed attacks on the territory of Member States in future, as occurred in Ukraine. In such a case, Member States could invoke the mutual assistance clause in Article 42(7) TEU to resort to self-defence.

V. **References**

Badillo Ángel and Félix Arteaga. «*El impacto estratégico* de la *desinformación en España*»*., Informe IBERIFIER,* Febrero 2024 (2024): 1-108. https://media.realinstitutoelcano.org/wp-content/uploads/2024/04/informe-iberifier-el-impacto-estratagico-de-la-desinformacion-en-espana.pdf.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

Baade, Björnstjern, «Fake News and International Law», *European journal of international law* 29.4 (2018): 1357-1376. http://www.ejil.org/article.php?article=2924&issue=146.

Biscop, Sven, and Jo Coelmont, «A Strategy for CSDP Europe's Ambitions as a Global Security Provider.» Egmont Institute (2010). https://www.egmontinstitute.be/a-strategy-for-csdp-europes-ambitions-as-a-global-security-provider/.

Cavaliere, Paolo, «From Journalistic Ethics to Fact-Checking Practices: Defining the Standards of Content Governance in the Fight against Disinformation», *The Journal of Media Law*, vol. 12, no. 2 (2020): 133-165, https://doi.org/10.1080/17577632.2020.1869486.

Centro Criptológico Nacional, Ministerio de Defensa, «Desinformación en el ciberespacio», BP/13 (2019): 1-50. https://www.ccn-cert.cni.es/es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/3549-ccn-cert-bp-13-desinformacion-en-el-ciberespacio/file.html.

Cipers, Samuel, Trisha Meyer and Jonas Lefevere, «Government Responses to Online Disinformation Unpacked» *Internet Policy Review*, vol. 12, no. 4 (2023): 1-19. DOI: 10.14763/2023.4.1736.

Corten, Olivier, «Discours de guerre, guerre de discours», *Revue interdisciplinaire d'études juridiques,* 2023/1 Volume 90 (2023): 155-176. https://doi-org.ezproxy-prd.bodleian.ox.ac.uk/10.3917/riej.090.0155.

D'Andrea, Alessia, Giorgia Fusacchia and Arianna D'Ulizia «Policy Review: Countering Disinformation in the Digital Age — Policies and Initiatives to Safeguard Democracy in Europe» *Information Polity*, vol. 30, no. 1 (2025): 82-91, https://doi.org/10.1177/15701255251318900.

Danylyuk, Oleksandr, «How to Resist Russia's Covert War Against the West», *International Center for Defence and Security*, Commentary, 26 June 2025 (2025). https://icds.ee/en/how-to-resist-russias-covert-war-against-the-west/.

De Cock Buning, Madeleine, «A multi-dimensional approach to disinformation : report of the independent High level Group on fake news and online disinformation», Luxembourg : Publications Office of the European Union (2018): 1-42. https://hdl.handle.net/1814/70297.

Engberg, Katarina, *The EU and Military Operations : A Comparative Analysis*. 1st ed., Routledge (2014). https://doi.org/10.4324/9780203381663.

Espaliú Berdud, Carlos, «The EU Response to the Paris Terrorist Attacks and the Reshaping of the Right of Self-Defence in International Law», *Spanish Yearbook of International Law* 20 (December) (2016): 183-207. https://www.sybil.es/sybil/article/view/1391.

Espaliú Berdud, Carlos, «Legal and Criminal Prosecution of Disinformation in Spain in the Context of the European Union», *Profesional de la información* 31 (3) (2022): 1-14. https://doi.org/10.3145/epi.2022.may.22.

Espaliú Berdud, Carlos, «Use of Disinformation as a Weapon in Contemporary International Relations: Accountability for Russian Actions Against States and International Organizations», *Profesional de la información* 32 (4) (2023): 1-19. https://doi.org/10.3145/epi.2023.jul.02.

European Parliament. «The fight against disinformation and the right to freedom of expression». Policy Department for Citizens' Rights and Constitutio-

nal Affairs Directorate-General for Internal Policies PE 695.445 – July 2021. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695445/IPOL_STU(2021)695445_EN.pdf

Fonseca-Morillo, Francisco, «Prólogo: La Europa que protege, de la teoría a la práctica gracias al pensamiento crítico y la alfabetización digital», *Revista de estilos de aprendizaje*, v. 13, n. 26 (2020): 1-3. https://doi.org/10.55777/rea.v13i26.2593.

Gobierno de España. Presidencia del Gobierno. «Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional. Propuestas de la sociedad civil» (2022): 1-297. https://www.dsn.gob.es/sites/default/files/2025-02/LUCHA%20CONTRA%20LAS%20CAMPA%C3%91AS%20DE%20DESINFORMACI%C3%93N%202022%20.pdf.

Hamilton, Tomas, «Defending Ukraine with EU Weapons: Arms Control Law in Times of Crisis», *European Law Open* 1, no. 3 (2022): 635-59. https://doi.org/10.1017/elo.2022.35.

Hénin, Nicolas, «FIMI: Towards a European Redefinition of Foreign Interference», April 2023. EU DisinfoLab. https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf.

Hollis, Duncan, «The Influence of War; The War for Influence», *Temple International and Comparative Law Journal* 32, no. 1 (Spring 2018): 31-46. https://sites.temple.edu/ticlj/files/2018/10/32.1_Article-5_Hollis.pdf.

Iosifidis, Petros, Nicholas Nicoli, «European Policy Strategies in Combating Digital Disinformation», in *Digital Democracy, Social Media and Disinformation*, 1st ed., vol. 1, Routledge (2021): 61-82. https://doi.org/10.4324/9780429318481-7.

Kachelmann, Matthias, and Wulf Reiners, «The European Union's Governance Approach to Tackling Disinformation – Protection of Democracy, Foreign Influence, and the Quest for Digital Sovereignty», *L'Europe En Formation*, November 13 (2023). https://doi.org/10.3917/eufor.396.0011.

Klamert, Marcus, «Article 4 TEU», in Manuel Kellerbauer, Marcus Klamert, and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (New York, 2019; online edn, Oxford Academic), https://doi.org/10.1093/oso/9780198759393.003.7.

Kmec, Vladimir, «CSDP Machinery and Peacebuilding», *EU Missions and Peacebuilding*, 1st ed., vol. 1, Routledge (2022): 45-72, https://doi.org/10.4324/9781003198901-3.

Kobernjuk, Anna, and Agnes Kasper, «Normativity in the EU's Approach towards Disinformation», *TalTech Journal of European Studies*, vol. 11, no. 1 (2021): 170-202, https://doi.org/10.2478/bjes-2021-0011.

Kudrna, Jan, «The possibilities of combating so-called disinformation in the context of the European Union legal framework and of constitutional guarantees of freedom of expression in the European Union Member States», *International Comparative Jurisprudence (Online)* 8.2 (2022): 138-151. https://doi.org/10.13165/j.icj.2022.12.002.

Loik, Ramon, et Madeira, Victor, «European Union Strategy and Capabilities to Counter Hostile Influence Operations», in: Holger Mölder, Vladimir Sazonov, Archil Chochia, Tanel Kerikmäe (eds) «The Russian Federation in Global

Knowledge Warfare. Contributions to International Relations» (Springer, Cham 2021:247-264). https://doi.org/10.1007/978-3-030-73955-3_13.

Mangas Martín, Araceli, «Guerra en Ucrania: perspectiva jurídico-internacional», *Actualidad Jurídica Uría Menéndez*, 60 (2022): 9-25. https://www.uria.com/documentos/publicaciones/8189/documento/ajum60art.pdf?id=13167&forceDownload=true.

Pamment, James, «The EU's Role in Fighting Disinformation: Taking Back the Initiative», *Policy File*, Carnegie Endowment for International Peace — US (2020): 1-23. https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf.

Proto, Lucas, Paula Lamoso-González and Luis Bouza García «The Great FIMI Pivot: How the EU's Fight Against Disinformation Is Being Reframed by the European External Action Service», *Media and Communication (Lisboa)*, vol. 13 (2025). https://doi.org/10.17645/mac.9474.

Ramopoulos, Thomas, «Article 42 TEU», in Manuel Kellerbauer, Marcus Klamert, and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (New York, 2019; online edn, Oxford Academic), https://doi.org/10.1093/oso/9780198759393.003.53.

Rasi, Aurora, «Providing Weapons to Ukraine: The First Exercise of Collective Self-Defence by the European Union?» *European papers (Online. periodico)* 9.1 (2024): 397-422. https://www.europeanpapers.eu/e-journal/providing-weapons-ukraine-first-exercise-collective-self-defence-european-union.

Renda, Andrea, «The Legal Framework to Address 'Fake News': Possible Policy Actions at the EU Level», *Policy File*, Centre for European Policy Studies (2018): 1-33. https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA(2018)619013_EN.pdf.

Schmitt, Michael «Providing arms and materiel to Ukraine: neutrality, Co-belligerency, and the use of force», *Article of war,* Lieber Institute, West Point, 7 March 2022 (2022). https://lieber.westpoint.edu/ukraine-neutrality-co-belligerency-use-of-force/.

Seijas, Raquel, »Las soluciones europeas a la desinformación y su riesgo de impacto en los derechos fundamentales», *IDP, Revista de internet, derecho y política*, n. 31 (2020): 1-14. https://raco.cat/index.php/IDP/article/view/373664/467277.

Shao, Chengcheng, Giovanni Luca Ciampaglia, Onur Varol, Kai-Cheng Yang, Alessandro Flammini & Filippo Menczer, « The spread of low-credibility content by social bots»., *Nature Communications* 9, 4787 (2018): 1-9. https://doi.org/10.1038/s41467-018-06930-7.

Suárez-Serrano, Chema, «From bullets to fake news: Disinformation as a weapon of mass distraction. What solutions does international law provide?», *Spanish Yearbook of International Law*, v. 24 (2020): 129-154. https://www.sybil.es/sybil/article/view/149.

Svicevic, Marko, «European Union Military Missions and the War in Ukraine: Moving beyond the Jus Ad Bellum Framework», *Polish Review of International and European Law (Online)*, vol. 13, no. 1 (2024): 89-117. https://doi.org/10.21697/2024.13.1.04.

Wardle, Claire and Hossein Derakhshan, «Information disorder. Toward an interdisciplinary framework for research and policymaking». Council of Eu-

rope (2017): 1-109. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.

Wardle, Claire, Rasmus Kelis Nielsen, Alexios Mantzarlis y Clara Jiménez Cruz, «Seis puntos claves del informe sobre desinformación del grupo de expertos de la Comisión Europea», Maldita, 12 marzo 2018. https://maldita.es/maldita/20180312/seis-puntos-claves-del-informe-sobre-desinformacion-del-grupo-de-expertos-de-la-comision-europea.

Sobre el autor

Carlos Espaliú ha sido becario de investigación del Ministerio de Educación (1995-1998); profesor de la Universidad de Navarra (1998-2000); Letrado de la Corte Internacional de Justicia (2000-2006); investigador Ramón y Cajal en la Universidad de Córdoba (2007-2012) ; profesor, vicedecano de la Facultad de Derecho y Director del Instituto Carlomagno de Estudios Europeos en la Universitat Internacional de Catalunya (2012-2018); Catedrático de Derecho Internacional Público y de la Unión Europea, Secretario General, así como Investigador Principal del Grupo de Seguridad, Gestión de Riesgos y Conflictos (SEGERICO) y Director del Centro de investigación en Seguridad, Estado de Derecho y Altas Tecnologías, en la Universidad Nebrija de Madrid (2018-2024). Desde 2024, es Catedrático de Derecho Internacional Público, Relaciones Internacionales y Derecho de la Unión Europea de la Universidad CEU Fernando III en Sevilla. Asimismo, es Research Fellow en el Las Casas Institute, Blackfriars Hall, University of Oxford y profesor visitante de la Universidad para la Paz de las Naciones Unidas, en Costa Rica. También cuenta con tres sexenios de investigación del CNEAI. En materia de derechos humanos, entre otros trabajos, ha coordinado en *Cuadernos Europeos de Deusto,* el Núm. 02 (2019). Monográfico. Identidad Europea: raíces y alcance.

About the author

Carlos Espaliú was a research fellow at the Ministry of Education (1995-1998); professor at the University of Navarra (1998-2000); Legal Officer at the International Court of Justice (2000-2006); Ramón y Cajal researcher at the University of Córdoba (2007-2012); professor, vice dean of the Faculty of Law, and director of the Charlemagne Institute of European Studies at the International University of Catalonia (2012-2018); Professor of Public International Law and European Union Law, Secretary General,

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 74/2026, Bilbao, págs. 105-141
doi: https://doi.org/10.18543/ced.3484 • https://ced.revistas.deusto.es

Principal Investigator of the Security, Risk and Conflict Management Group (SEGERICO), and Director of the Research Center for Security, Rule of Law, and High Technologies at Nebrija University in Madrid (2018-2024). Since 2024, he has been Professor of Public International Law, International Relations, and European Union Law at CEU Fernando III University in Seville. He is also a Research Fellow at the Las Casas Institute, Blackfriars Hall, University of Oxford, and a visiting professor at the United Nations University for Peace in Costa Rica. He has also been accredited with three six-year periods of research by the CNEAI. In the field of human rights, among other works, he has coordinated *Deusto Journal of European Studies*, No. 02 (2019): Special issue. European Identity: Roots and Scope.