Use of disinformation as a weapon in contemporary international relations: accountability for Russian actions against states and international organizations

Carlos Espaliú-Berdud

Nota: Este artículo se puede leer en español en:
https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/87196

Recommended citation:

Espaliú-Berdud, Carlos (2023). "Use of disinformation as a weapon in contemporary international relations: accountability for Russian actions against states and international organizations". *Profesional de la información*, v. 32, n. 4, e320402.

https://doi.org/10.3145/epi.2023.jul.02

Article received on November 28th 2022
Approved on April 18th 2023

Carlos Espaliú-Berdud
https://orcid.org/0000-0003-4441-6684

Universidad Antonio de Nebrija
Santa Cruz de Marcenado, 27
28027 Madrid, Spain
cespaliu@nebrija.es

Abstract

We have chosen to study international responsibility for carrying out disinformation campaigns, aiming to assess the importance and progress that the use of disinformation campaigns has obtained in contemporary international society as a geopolitical weapon, much like other well-established means such as the use of force. We focus on the situation with Russia because it has become apparent not only to specialized researchers but also to all citizens through the mainstream media that Russia has used disinformation campaigns to cloak its invasion of Ukraine in a smoke cloud of lies and half-truths. Thus, we found that, in the case of the Russian disinformation campaigns, the full circle of the accountability relationship has been completed. The Russian state has been accused of or blamed for carrying out these disinformation campaigns. The violation of certain international obligations has been reported, and it has been held accountable or even sanctioned for this. In light of these findings, it can be concluded that disinformation campaigns are becoming increasingly important as a tool of geopolitics or international relations, either on their own or in conjunction with other, more classic weapons in international society, such as the age-old use of force.

Keywords

International accountability; Disinformation; Cyberattacks; Fake news; Use of force; Countermeasures; International wrongful acts; Sanctions; International relations; European Union; *NATO*; Rusia; Ukraine.

1. Introduction

The prominence of cyberattacks, as a regular feature at the forefront of contemporary forms of crime around the world, is no longer a novel effect. Most probably, the readers of this article themselves have suffered some form of cyberattack aimed at financial gain at one time or another, in person or at the institutions where they work. In parallel to these cyberattacks, which alter the computer systems of those affected –whether individuals, companies, or public institutions– for financial motives, other attacks aimed at altering public opinion and thus damaging the democratic function of both states and international organizations are increasingly taking place, and thus becoming part of international relations and the geopolitical landscape.

The latter type of action has come to be known as "disinformation" campaigns. For the moment, we can define this expression briefly as

> "[...] the intentional dissemination of inaccurate information that seeks to undermine public confidence, distort facts, convey a certain way of perceiving reality, and exploiting vulnerabilities with the aim of destabilizing" (**Olmo-y-Romero**, 2019, p. 4)

since, in the following section, we will delve more deeply into this concept and try to distinguish it from related ideas.

In this regard, it should be emphasized that, although deception techniques have always been employed for the purposes of politics or war (*Centro Criptológico Nacional*, 2019, p. 5), nowadays their danger and scope have increased owing to the technological revolution that has taken place worldwide, making them a serious global risk (**Shao** *et al*., 2018, p. 2). Furthermore, experts have pointed out various factors that are contributing to the proliferation of these disinformation campaigns: First, it is necessary to highlight their high level of effectiveness owing to current technological capabilities and to the fact that, typically, they affect social vulnerabilities that already exist in the society being attacked, or that, like weeds among the wheat, elements of the illegitimate disinformation are inserted into legitimate means of social and political communication, thereby increasing their plausibility (*Centro Criptológico Nacional*, 2019, pp. 5-7).

Second, their recurrence could be explained by the difficulty of determining who is responsible for the campaigns and by the obstacles to figuring out the connection between the orchestrated campaign and the influence it has had in changing public opinion about the entities that were victims of the attacks (*ibid.*).

Third, the replacement of traditional media by social networks as reliable information channels weakens receivers' defensive capabilities because, as several experts have warned, one consequence of the social network empire is that, when compiling stories from multiple sources, the focus is on the story and not as much on its source, as well as because endorsements and recommendations –rather than the traditional gatekeepers of established media or ingrained reading habits– guide readers on social networks (*ibid.*; **Messing** *et al.*, 2012, p. 3; **Wardle** *et al.*, 2017, p. 12).

Finally, the scope and dangerousness of disinformation campaigns have escalated owing to the intrinsic difficulty faced by democratic societies when it comes to legally prosecuting these hostile actions against our societies (**Iosifidis** *et al.*, 2020, p. 64), unlike with other more unambiguously offensive conduct, such as armed attacks, terrorist actions, or even computer attacks on systems or hacks. Indeed, it is difficult to combat disinformation without at the same time attacking the fundamental principles of democratic states and societies, such as freedom of expression and opinion, which underpin the fundamental individual rights of both nationals and foreigners.

In the context of this monograph, which is dedicated to the importance of disinformation in international relations, we would like to emphasize that states, and some international organizations such as the European Union (EU) itself, have increasingly acknowledged having been subjected to massive disinformation campaigns, especially in electoral or political contexts, either by internal groups, as in the recent election campaigns in Germany (**Delcker**; **Janosch**; 2021), or by third countries, with the specific objective of discrediting and delegitimizing elections (*United States Senate Select Committee on Intelligence*, 2017). For example, as recently as September 2021, the *EU High Representative for Foreign Affairs and Security Policy*, Josep Borrell, said that some member states had observed malicious cyber activity, referred to collectively as "ghostwriter," which endangered integrity and security and had linked them to the Russian state. The *High Representative* stated that these malicious cyber activities targeted EU parliamentarians, government officials, politicians, and members of the press and of EU civil society by accessing computer systems and personal accounts and stealing data. Borrell concluded that these activities were contrary to the norms of responsible state behavior in cyberspace that had been endorsed by all members of the *United Nations* and that such activities were intended to undermine the democratic institutions and processes of the EU member states,

> "[...]including by enabling disinformation and information manipulation, in particular by enabling disinformation and manipulation of information" (*Council of the European Union*, 2021).

Naturally, as soon as these disinformation campaigns began to be detected, international organizations and states tried to put in place the means to counteract them both legally and through the implementation of other more informal means (**Espaliú-Berdud**, 2022, pp. 4-6). For example, in March 2015, the *European Council* required the *EU High Representative for Foreign Affairs and Security Policy* to prepare an action plan on strategic communication (*European Council*, 2015, point 13), which led to the creation of the *East StratCom Task Force*, operational since September 2015, which is part of the *Strategic Communications and Information Analysis Division* of the *European External Action Service*. Its main mission is to develop communication elements and information campaigns aimed at better explaining EU policies in the countries to the east. For example, one of the star projects of the *East StratCom Task Force* was the 2015 creation of *EUvsDisinfo*, which consists of a portal and a set of databases designed to better anticipate, address, and respond to current disin-

> Like weeds among the wheat, elements of the illegitimate disinformation are inserted into legitimate means of social and political communication, thereby increasing their plausibility (*Centro Criptológico Nacional*, 2019, pp. 5-7)

formation campaigns from the Russian Federation that affect the EU, its member states, and neighboring countries.

> It is difficult to combat disinformation without at the same time attacking the fundamental principles of democratic states and societies, such as freedom of expression and opinion, which underpin the fundamental individual rights of both nationals and foreigners

Moreover, one must remember that the severe acute respiratory syndrome coronavirus 2 (SARS-COV-2) pandemic, more popularly known as coronavirus disease 2019 (COVID-19), has been accompanied by powerful disinformation campaigns, casting an even longer shadow over the situation already described, reaching a point where the *World Health Organization* has described the situation as an "infodemic" (*World Health Organization*, 2019, p. 34).

Thus, for example, in a joint communication in June 2020, the *European Commission* and the *High Representative of the Union* warned that, among the many harmful elements of the pandemic, some foreign actors and certain third countries, including Russia, had launched disinformation campaigns about Covid-19 in the EU, in its neighborhood, and globally with the aim of undermining democratic debate and exacerbating social polarization (*European Commission* and *High Representative of the European Union for Foreign Affairs and Security Policy*, 2020, p. 4). Subsequently, these Russian-based disinformation campaigns were documented in detail as the pandemic dragged on (*European External Action Service*, 2021).

However, it should be noted that, insofar as disinformation companies are sponsored by other states and form part of a hybrid threat from abroad, they could come to be considered a security threat (**Baade**, 2018, p. 1358), and the responses to such situations can be found within the framework of public international law, in particular Chapter VII of the *United Nations Charter*. Thus, as Suárez-Serrano points out:

> "If a disinformation campaign reaches the capacity to put peace and security at risk, it should be formally designated as a threat, and the responsible state might be sanctioned in the way considered by the *UN Security Council*" (**Suárez-Serrano**, 2020, p. 140).

Unfortunately, the invasion of Ukraine in February 2022 is proving the plausibility of these hypotheses. In fact, let us recall that the Russian authorities devised a series of arguments as justification for the invasion, which they called, as is well known, a "special operation" –an action to put an end to the massacres of pro-Russian separatists in the Ukrainian regions of the Dombas because they considered it necessary to overthrow the legitimate Ukrainian government for being "neo-Nazi," and to protect both Russia and Ukraine from a possible rapprochement to the EU and the *North Atlantic Treaty Organization* (*NATO*); **Corral-Hernández**, 2022, p. 6). As the war has unfolded, other campaigns defending the *Kremlin*'s narratives about the war in Ukraine –such as denying the Bucha massacre and inciting fear among European citizens about how sanctions against Russia would ruin their lives, etc.– have been detected (**Alaphilippe** *et al*., 2022).

It is therefore becoming less and less over-the-top to point out, as many observers have already done, that Russia is now once again using "active measures", a term borrowed from the lexicon of the *Soviet Union's Committee for State Security* (*KGB*) during the Cold War (**Colom-Piella**, 2020, p. 474) to describe a form of political warfare involving, among other things, the use of fake news, as well as forged letters disseminated on social media, to influence public opinion in target countries (**Lanoszka**, 2019, p. 227).

However, in spite of the confirmation of all these data and despite the fact that many years have passed since these strategic disinformation campaigns began to be detected, there are experts who question the reach of these campaigns. For example, Professor Lanoszka has stated that

> "[...] the strategic effects of international disinformation campaigns are exaggerated" (**Lanoszka**, 2019, p. 229).

Similarly, Andrew Dawson and Martin Innes point out that

> "[...] we need to be wary of over-attributing any causal effects to even the most sophisticated disinformation campaign" (**Dawson**; **Innes**, 2019, p. 245),

as well as that

> "[...] there is actually remarkably little robust evidence that such disinforming communications have a discernible measurable impact upon how the majority of people think, feel or act" (*ibid.*, p. 255).

For them, therefore,

> "[...] it is more appropriate to argue that disinformation has more impact in shaping the issues we collectively think about, than what we individually think" (*ibid.*).

Hence, we propose examining the possible relationship of international responsibility arising from the use of disinformation campaigns as a means to shed light on this debate, namely to determine the relevance and scope of the use of disinformation campaigns in international society as a tool of international relations. Recall that responsibility is the legal institution, essential to any legal system, including the international one, that demands that the breach of any

obligation existing between two or more parties creates a new obligation, that of repairing the damage caused by that breach or at least restoring the legal situation to the moment prior to the breach. The legal system of responsibility in international law –which has been clarified mainly through codification and progressive development carried out by the *International Law Commission* (*ILC*), a subsidiary body of the *General Assembly of the United Nations* (*UN*), since 1949– involves making a claim against the acting party that has caused the act so that they will take responsibility for the consequences of their actions and to do everything possible to restore the legal situation to its original state, for example, by repairing the damage caused, etc.

> "The Russian authorities devised a series of arguments as justification for the invasion, which they called, as is well known, a "special operation" –an action to put an end to the massacres of pro-Russian separatists in the Ukrainian regions of the Dombas because they considered it necessary to overthrow the legitimate Ukrainian government for being "neo-Nazi"

Thus, returning to the context of disinformation campaigns, if, in addition to indicating the state that has used such means, the affected states have already proceeded to hold the other state internationally responsible and, as appropriate, to claim reparations from it, we could argue that disinformation campaigns are already considered to be a true wrongful act whose execution generates the normal consequences attributable to other wrongful acts in international law, such that they have already reached a certain maturity as a legal institution in this system. In this way, they would have already moved beyond the initial stage in which they are the object of mere cross-accusations between states without any major consequences apart from serving as another possible form of international wrongdoing –hence, their use as a geopolitical tool, or weapon, but one that is already sufficiently known and targeted by adversaries.

In particular, we plan to study the case of disinformation campaigns attributed to Russia because, since this state recently engaged in the use of armed force when invading Ukraine, examining Russian disinformation campaigns will allow us to deepen our understanding of the importance of using these tools across the spectrum of their geopolitical usage –from political or economic rivalry with other nations to hostility or war. In addition, the fact that this is a real war that is still going on today gives the issue high visibility, which triggers reactions, narratives, and actions from other international actors beyond those strictly involved.

To examine the handling of Russia's possible international responsibility for violating international obligations by using disinformation campaigns, I believe that we should follow the structure of the rules contained in the *ILC*'s draft articles on *International Accountability of States For Internationally Wrongful Acts*, submitted for consideration by the *UN General Assembly* in 2001. It should be remembered that, without proposing a pact, the *General Assembly* submitted the draft for the consideration of the states in 2002 (*United Nations*, 2002). Of course, as they are not part of a pact, these rules are not binding in themselves, although some of them would be binding because they reflect customary international law on the subject. After article 1 has established the basic rule on the subject, namely that

> "every internationally wrongful act of a State entails its international accountability,"

article 2, to be exact, of the aforementioned draft establishes that an internationally wrongful act occurs when conduct consisting of an act or omission is attributable to the state under international law and constitutes a breach of an international obligation. Likewise, according to the rules of the regime of international responsibility of states for the committing of wrongful acts, if it is demonstrated that the conduct of the state can be considered to be a wrongful act, and there are no circumstances in the specific case that exclude the wrongfulness of the particular act, a new legal relationship will be established between the holder of the obligation breached and the state that has carried out the breach, which will essentially consist of the obligation to put an end to the wrongful act, to give guarantees of non-repetition, and to make full reparation for the damage caused by the internationally wrongful act.

To this end, after a section devoted to an in-depth study of the concept of disinformation, we will analyze how the conditions for attributing unlawful behavior to Russia have been justified in practice in the third section. In the fourth section, we will address the question of the reality of handling the target element of international responsibility as a possible breach of an international obligation. In the fifth section, we will examine the scenario of possible cases of the states or international organizations concerned the Russian state responsible once those other states or international organizations have established or, at least, imputed its perpetration of the breach of the international obligations.

Primarily, given the nature of the journal in which this article is included, we will mainly follow the methodology of the legal sciences, analyzing primary sources such as international treaties; the resolutions of international organizations, such as those of bodies and agencies of the *UN*, the *CE*, the *Council of Europe*, and *NATO*; the case law of international courts on the subject; and the treatment of the question of international mechanisms for the protection of human rights or the application of applicable international treaties. In parallel, as regards secondary sources, we will make use of the most relevant and recent doctrinal developments on disinformation and related concepts, both in Spain and internationally, as well as those related to the use of "disinformation" as a tool or weapon in the international relations sphere.

2. The concept of disinformation and distinguishing it from related notions

In an era of infosaturation, or information overload, and of informational banalization, or content inconsequentiality (**Valverde-Berrocoso** *et al*., 2022), and one in which traditional media and journalists are replaced by the so-called horizontal media, such as social networks, where there is no screening and the propagator communicates directly with his audience (**Bernal-Hernández**, 2021, pp. 95-96), there are several information disorders with similar profiles that one must try to distinguish to delve deeper into the phenomenon that concerns us herein and shed more light on this matter for the reader. However, it should be noted that the task of distinguishing one type from another in this area is not simple, since, as Claire Wardle and Hossein Derakhshan warn,

> "[...] the complexity and scale of information pollution in our digitally-connected world presents an unprecedented challenge" (**Wardle**; **Derakhshan**, 2017, p. 10).

For example, these authors start with the generic classification of "information disorders", and focus on the distinction between "disinformation," "mis-information," and "mal-information." Thus, for Claire Wardle and Hossein Derakhshan, these are defined as follows:

> "*Dis-information*. Information that is false and deliberately created to harm a person, social group, organization or country.
> *Mis-information*. Information that is false but not created with the intention of causing harm.
> *Mal-information*. Information that is based on reality, used to inflict harm on a person, organization or country" (*ibid.*, p. 20).

Here, however, we will focus on distinguishing the terms most widely used in recent years and in the context of this article, without delving into the other terms that have undeniable connections with them in the framework of communication, such as "manipulation" techniques, which are a communicative and interactional practice in which the person who carries them out, as Teun Van Dijk points out, exercises control over other people, generally against their will or against their interests (**Van-Dijk**, 2006, p. 51). As an example of manipulation, Van Dijk cites a speech given by then Prime Minister of the United Kingdom, Tony Blair, in March 2003 to obtain the *British Parliament*'s approval for the British armed forces' participation in the Iraq war (**Van-Dijk**, 2010, p. 187). The term "control of the narratives" can also be considered similar to the ones we are considering here, both in its positive connotation referring to the surveillance activities carried out by public authorities or other social agents to prevent forms of criminality in cyberspace (**Altheide** 2004, pp. 229-234; **Hetland**, 2012, p. 9) as well as in its negative connotation as the ways of influencing the discourses that are dumped onto these communicative channels by other agents with intention to dominate, manipulate, etc.

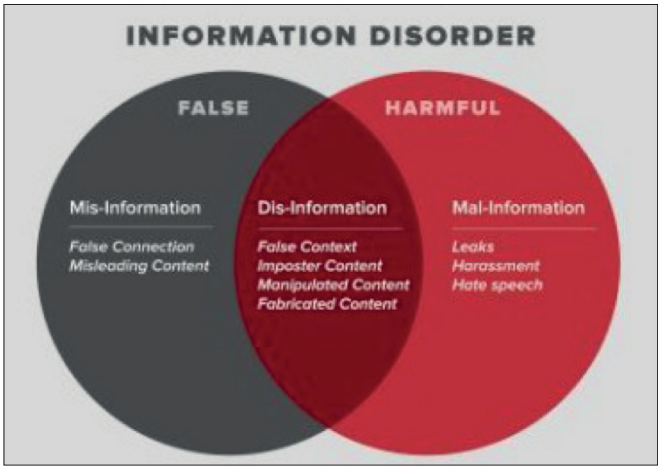

Figure 1. Informational disorder according to Claire Wardle and Hossein Derakhshan (**Wardle**; **Derakhshan**, 2017, p. 20)

Starting with the concept of "disinformation" itself, which has been defined in the introduction, it is worth noting the concurrence of three elements:

- lack of rigor or falsehood in the information;
- conscious dissemination of that flawed information; and
- intention to cause harm in the recipients or in the victim society itself (**Olmo-y-Romero**, 2019, p. 4; **Wardle**; **Derakhshan**, 2017, p. 5; **Egelhofer**; **Lecheler**, 2019, p. 102).

Thus, to coin our own definition, for us disinformation is orchestrated dissemination of untruthful news or data through any type of communication channels, whether traditional –printed press, radio, television– or horizontal –social networks, etc.– with the intention of obtaining an economic, social, or strategic benefit, or of harming rivals, whether individuals, societies, institutions, or states.

By way of illustration, let us indicate the methodology that some of the most serious disinformation campaigns, aimed at destabilizing the targeted society, tend to follow. First, we proceed to the analysis and detection of social and political vulnerabilities of the victim entity. Second, transmedia narratives are developed, which will be disseminated through various communication chan-

> "Disinformation campaigns are already considered to be a true wrongful act whose execution generates the normal consequences attributable to other wrongful acts in international law"

nels. Third, their own media network is established, and finally, they proceed to create automated distribution channels (*Centro Criptológico Nacional*, 2019, pp. 17-19).

In contrast, "fake news" has a smaller quantitative scope than "disinformation" (**Rodríguez-Pérez**, 2019, p. 65); it is specific false news items, false or falsified messages, half-truths, and hoaxes, though consciously transmitted for economic, political, social, strategic, or other benefits, or to damage the reputation or image of an adversary or enemy.

For us, therefore, the difference between "fake news" and "disinformation" is in the numerical dimension –in the scale on which they are used. Thus, disinformation is carried out through campaigns of dissemination of false news or hoaxes, seeking, as Pilar Bernal warns,

> "[...] to shift the decision-making process and thus alter the perception of national and international publics and audiences" (**Bernal-Hernández**, 2021, p. 97).

This relationship and the quantitative difference are clearly seen, in my opinion, in Julio Montes' account of the contribution of the Russian television channel *RT* to the Russian strategic effort:

> "Their mission is not to misinform with occasional hoaxes on a recurring basis, as other 'fake' websites can do, but rather it is all part of a global and long-term action with a political objective. As the media weapon of Putin's government that they are, they have a propagandistic purpose behind them. They are an example of disinformation in a broader and more far-reaching sense: a mixture of realities, half-truths and rumors on issues that have direct stakes for Russia" (**Montes**, pp. 42-43).

Indeed, Julio Montes provides us with a real and practical example of a disinformation campaign, closely linked to the subject of this article: the use of the television channel *RT* to support Russian interests in their invasion of Ukraine in 2022. For Julio Montes, *RT*'s disinformative campaign in Spanish

> "[...] had begun before the first shot was fired. For months, Russia and its media outlets denied that there was a plan to invade Ukraine. It was all 'conspiracy theories'" (*ibid*. p. 42).

Thus, for this author, months before what was ultimately an invasion of the territory of neighboring Ukraine, the Russian "journalists" at *RT* in Spanish

> "[...] sought to discredit the content that warned of the approach of Russian troops to Ukraine and the information that warned of a possible invasion by Russia:
> 'Of course, January will come and then February and March, 2022 will end, and I'm sure in the media you'll still read that the invasion is imminent. Those who warn again and again of an imminence that never comes do not do so out of ignorance, but rather because they have calculated it perfectly'" (*ibid.*).

Montes also notes that, on February 20, a few days before the imminent invasion, *RT*, quoting the Russian government, spoke of the "myth of the invasion" (*ibid.*). However, Montes warns,

> "The day after the Russian attack, on Friday, February 25, *RT* spoke of 'an operation' to 'safeguard the security of millions of people living in Dombas.' Despite months of reports about this possible attack, the RT presenter said that 'it had been a surprise'" (*ibid.*).

Another example of disinformation in practice, in which Russia also played a starring role, was detected by the *UK Government*, which uncovered evidence of *TikTok* influencers being paid to amplify pro-Russian narratives following the 2022 invasion of Ukraine (*Organisation for Economic Co-operation and Development*, 2022, p. 3).

Finally, regarding the term "propaganda," we must also draw attention to its similarity to the term "disinformation." Indeed, as Alejandro Pizarroso-Quintero argues:

> "Propaganda, in the field of social communication, consists of a process of dissemination of ideas through multiple channels with the purpose of promoting in the target group the objectives of the sender not necessarily favorable to the receiver; it implies, then, a process of information and a process of persuasion" (**Pizarroso-Quintero**, 1991, p. 147).

Along these lines, Randal Marlin specifies that, in general, propaganda involves some kind of deception or prevents the audience from rationally and knowledgeably evaluating the message that the communicator wishes to convey (**Marlin**, 2014, pp. 191-92). Although there is no doubt that it had been used before, experts agree that it was used extensively during the First World War (**Bernal-Hernández**, 2021, p. 94). After this, a theory of propaganda was outlined for the first time (**Pizarroso-Quintero**, 1991, p. 151), probably based on the work of the American political scientist and sociologist Harold Dwight Lasswell *Propaganda Technique in the World War*, published in 1927, in which he prophetically warned of the importance of this tool for political purposes.

> "As an example of manipulation, Van-Dijk cites a speech given by then Prime Minister of the United Kingdom, Tony Blair, in March 2003 to obtain the *British Parliament*'s approval for the British armed forces' participation in the Iraq war"

In short, as can be seen, all these cases involve similar concepts, which have appeared at different times and have gained notoriety at certain moments, referring to the use of different communication tools to disseminate biased content for specific purposes, though for the purposes of this article, we emphasize the political or strategic purpose.

We would not want to close this section without noting the damage that these errors, now widespread, are producing in journalistic work (**Egelhofer**; **Lecheler**, 2019, p. 112), which as highlighted by Rodríguez-Pérez:

> "[...] consists of informing so that knowledge becomes flesh in society" (**Rodríguez-Pérez**, 2019, p. 67) .

In any case, we must point out that, in this paper, out of all the phenomena of communication disorders described, we will mainly talk about "disinformation" because it is the one that best represents the activities of media indoctrination carried out in an orchestrated manner by Russian government bodies to destabilize their rivals. Moreover, we will use the term "disinformation" in a generic way, without excessive concern for terminological precision, which would be impractical, in relation to the similar concepts we have just discussed, such as "fake news" or "propaganda." Methodological choice, on the other hand, is not unusual in official texts and documents –for example, in the *Joint Statement on Freedom of Expression and Fake News, Disinformation, and Propaganda* by the *UN* Special Rapporteur on Freedom of Opinion and Expression, the *Representative of the Organization for Security and Cooperation in Europe for Freedom of the Media*, the Special Rapporteur of the *Organization of American States for Freedom of Expression*, and the Special Rapporteur of the *African Commission on Human and Peoples' Rights for Freedom of Expression and Access to Information* (*United Nations Special Rapporteur on Freedom of Opinion and Expression et al.*, 2017).

3. Attribution to a state

Generally speaking, as we said in the introduction, we understand that the rules contained in the aforementioned *ILC* draft articles on the responsibility of states for internationally wrongful acts should be applied to cases of attribution of international responsibility to a particular state for using disinformation campaigns against other states or international organizations.

According to article 2 of the draft articles, one of the two basic conditions for establishing the international responsibility of a state is that the conduct in question is attributable to that state under international law. In this sense, the general rule is that the only conduct attributable to the state in the international sphere is that of its public, executive, legislative, or judicial bodies, at any level of the administration, or that of others acting under the direction or control or at the instigation of those bodies –that is, as agents of the state. In contrast, the conduct of private individuals or non-state entities cannot be attributed to the state under international law. However, article 8 of the draft provides that there may be circumstances in which such conduct may be attributable to the state because there is a specific factual relationship between the person or entity engaging in the conduct and the state. In fact, article 8, which reflects one of the rules of the draft that according to the *International Court of Justice* is considered common law (*International Court of Justice*, 2007a, p. 207, para. 398), provides that, according to international law, the following shall be considered an act of a state:

> "The conduct of a person or group of persons [...] if that person or that group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."

As regards the specific problem of the conduct of state-owned or state-controlled corporations or enterprises, which is of particular interest to us when it comes to shedding light on the situation of the media, the *ILC* commentary to the draft articles notes that the fact that the state originally created a corporation, whether by special law or otherwise, does not constitute a sufficient basis for attributing the subsequent conduct of that entity to the state (*International Law Commission*, 2001, p. 50). For the *ILC*, corporations,

> "[...] although owned and in that sense subject to the control of the State, are considered to be separate, *prima facie* their conduct in carrying out their activities is not attributable to the State unless they are exercising elements of governmental authority within the meaning of article 5" (*ibid.*)

That is to say, if they are empowered by the law of that state to exercise the attributions of powers of the public authority (*ibid.*, p. 44).

Moving these rules into the arena of disinformation campaigns, we understand that those orchestrated by media or entities that, de facto, acted on the instructions or under the direction or control of the state concerned when such conduct is observed would be attributable to the state concerned, whether or not such entities are state-owned. In this regard, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* warns, for example, that,

> "[...] States may contract with a private company to conduct cyber operations. Similarly, States have reportedly called upon private citizens to conduct cyber operations against other States or targets abroad (in a sense, 'cyber volunteers')" (**Schmitt**, 2013, p. 32).

For the authors of this work, these situations must be distinguished from those in which certain citizens ("hacktivists" or "patriotic hackers"), on their own initiative, carry out cyber operations (*ibid.*, p. 33).

This would be the theory, but in reality, attributing disinformation campaigns to a state is difficult (**Dawson**; **Innes**, 2019, p. 253; **Lehmann**, 2022) because it is technically possible to distribute information on the Internet without leaving tra-

ces of its origin, and because sometimes several entities are used at the same time to spread the information, thus responsibility becomes less clear. For example, in the case of the Russian state, one can demonstrate close connections between the state and media outlets such as *Russia Today* (*RT*) and *Sputnik*, which appear to be funded by the Russian government (**Baade**, 2018, p. 1361). However, this would most likely not be enough for their actions to be attributable to the Russian state; it would be necessary to prove that the state is de facto directing their actions when they orchestrate disinformation campaigns. By way of illustration, let us note that Björnstjern Baade, the editor-in-chief of *Russia Today*, being one of the 300 journalists decorated by Vladimir Putin for the news coverage of the conflict in Crimea would not be sufficient to attribute the news that appeared in that media outlet to the Russian state (**Baade**, 2018, p. 1362).

> "Disinformation is orchestrated dissemination of untruthful news or data through any type of communication channels, whether traditional –printed press, radio, television– or horizontal –social networks, etc.– with the intention of obtaining an economic, social, or strategic benefit, or of harming rivals, whether individuals, societies, institutions, or states"

In the same vein, in the report *Doppelganger: Media Clones Serving Russian Propaganda*, published in September 2022 and created by researchers from the *EU DisinfoLab* platform –an independent non-governmental organization (NGO) focused on researching and fighting disinformation campaigns targeting the EU, its member states, its core institutions, and its fundamental values– after having stated that a disinformation campaign of which many elements pointed to the involvement of Russian-based actors had been uncovered, it ultimately warned that the research developed

> "[...] does not lead to a formal attribution to a specific actor." (**Alaphilippe** *et al*., 2022).

By way of illustration, it should be noted that, among these elements pointing to a Russian origin, it was specified that, in terms of infrastructure, the spoofed domain names were operated by the same actor, and some of these domains were purchased through the Russian Internet registrar. The fake videos were produced by computers with a Russian configuration, etc. (*ibid.*).

On the contrary, in some official documents of the states, such as some of those of the *US Senate*, certain disinformation campaigns carried out through certain Russian media outlets are attributed to the Russian state, so the leap has already been made. Indeed, according to the findings of the report *Russian Active Measure Campaigns and Interference in the 2016 US Election* prepared by the *United States Senate Select Committee on Intelligence* to investigate Russian intervention in the 2016 American election:

> "In 2016, Russian operatives associated with the St. Petersburg-based *Internet Research Agency* (*IRA*) used social media to conduct an information warfare campaign designed to spread disinformation and societal division in the United States" (*United States Senate*, 2020), vol. II, p. 73).

For the *Committee*, the *Russian Government*

> "[...] tasked and supported the *IRA*'s interference in the 2016 U.S. election" (*ibid*. p. 75),

and moreover, that data is consistent with the relationship evident to the *Committee* between *IRA* owner Yevgeniv Prigozhin and the *Kremlin*. Thus, despite Moscow's denials,

> "the direction and financial involvement of Russian oligarch Yevgeniy Prigozhin, as well as his close ties to high-level Russian government officials including President Vladimir Putin, point to significant *Kremlin* support, authorization, and direction of the *IRA*'s operations and goals" (*ibid.*).

In addition, we can see how, increasingly and more clearly, EU institutions are pointing the finger at certain foreign states when it comes to pinpointing the responsibility for disinformation campaigns perpetrated against the EU itself or against member states. For example, as already highlighted in the introduction to this article, on September 24, 2021, in his declaration, on behalf of the EU, on respect for democratic processes in the EU, the *EU High Representative for Foreign Affairs and Security Policy*, Josep Borrell, stated that some member states had observed malicious computer activities, collectively referred to as "ghostwriting," that endangered integrity and security, and they had been linked to the Russian state (*Council of the European Union*, 2021).

Likewise, the *Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation* (2020/2268(INI)), by the *European Parliament's Special Committee on Foreign Interference in All Democratic Processes in the European Union*, including Disinformation, unequivocally warned that:

> "[...] evidence shows that malicious and authoritarian foreign state and non-state actors, such as Russia, China and others, use information manipulation and other interference tactics to interfere in democratic processes in the EU" (*European Parliament*, 2022a, D).

It openly added that these attacks are part of a hybrid war strategy and represent a violation of international law (*ibid*). With that report in mind, a few weeks later the *European Parliament* adopted a resolution –*European Parliament Resolution of 9 March 2022 on Foreign Interference in All Democratic Processes in the European Union, Including Disinfor-*

mation (2020/2268(INI))– in which, after reiterating the statements contained in the aforementioned report (*European Parliament*, 2022b, E), it states even more strongly that:

> "[...] Russia has been engaging in disinformation of an unparalleled malice and magnitude across both traditional media outlets and social media platforms, in order to deceive its citizens at home and the international community on the eve of and during its war of aggression against Ukraine, which Russia started on 24 February 2022, proving that even information can be weaponised" (*European Parliament*, 2022b, C).

In the same line of blunt accusation, we bring up the joint statement of EU and US Ambassadors to Bosnia and Herzegovina from June 6, 2022. In it, shortly before the Russian ambassador addressed the Bosnian parliament, he warned, that, with respect to the Ukrainian conflict, the deputies were going to hear disinformation about the brutal invasion of Ukraine. To cite an example, it stated:

> "[...] You are likely to hear that Russia is protecting people from Nazism. These are outrageous lies. Moscow seeks to exploit the cultural and religious bonds that Russia shares with the Serb people to divert your attention from its crimes in Ukraine." (*European External Action Service*, 2022).

4. Violation of an international obligation

As in the previous section, following the rules of the *ILC* draft articles on *International Responsibility of States for Internationally Wrongful Acts*, after the analysis of whether it is possible to attribute certain disinformation campaigns to the Russian state, we will study the handling in international practice of Russia's possible violations of international obligations in this section.

Thus, we should note that, in the more or less thinly veiled accusations presented above that both private and official actors from states or international organizations have made against Russia, three types of international obligations allegedly violated by disinformation campaigns were indicated: interference in domestic affairs, violation of human rights, and security threats.

However, we should point out now that accusations of Russia being behind certain disinformation campaigns were usually accompanied by the accusation of having carried out cyberattacks against the states or international organizations in question. This is logical since, if the objective of the "aggressor" state is to destabilize and damage the "victim" state or international organization, in particular, as we shall see, in its internal democratic functioning, it will normally seek to achieve this end by various means simultaneously.

4.1. Interference in domestic affairs

As the *International Court of Justice* made clear in the *Nicaragua* case in 1986:

> "The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; although examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law" (*International Court of Justice*, 1986, p. 106, para. 202).

This confirmed that the prohibition against intervening in the domestic affairs of states was compulsory not just for the *United Nations* organization, as prescribed in article 2.7 of the *San Francisco Charter*, but rather for all states. In that landmark ruling, the *International Court of Justice* also addressed the substance of this principle, stating that it prohibits those interventions related to matters on which each state may, by virtue of its sovereignty, freely decide, and specified, among other issues, the freedom to choose a political, economic, social, and cultural system, as well as the formulation of its foreign policy (*International Court of Justice*, 1986, p. 108, para. 205). The *Court* added to these considerations that:

> "[...] Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State" (*ibid.*).

Let us recall that, in its *Resolution 2131 on December 21, 1965*, entitled "Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and Protection of Their Independence and Sovereignty," the *United Nations General Assembly* had already indicated that could be considered violations of that principle

> "[...] armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, [...]" (*Organization of the United Nations*, 1965).

In the context of this article, a disinformation campaign carried out by a state with the intention of destabilizing another state or an international organization must be considered an act of intervention in the domestic affairs of another state. Of course, if this were accompanied by other hostile elements, such as cyberattacks or the threat or use of force, that would increase its seriousness and, in such a case, the international responsibility of the state. Let us examine whether there have been actual cases in which specific disinformation campaigns have been considered acts of intervention in domestic affairs and how they have been dealt with.

In the *European Parliament Resolution of 9 March 2022* on foreign interference in all democratic processes in the European Union, including disinformation [*2020/2268(INI)*] –which we commented on previously mentioning the *Charter*

of the United Nations, in particular articles 1 and 2, and *Resolution 2131 (XX) of the United Nations General Assembly*, which condemns not only armed intervention but also any other form of interference or attempted threat against the personality of the state or against its political, economic, and cultural elements– information manipulation, of which Russia and China were accused, was considered a form of interference (*European Parliament*, 2022b, A and E).

> A disinformation campaign carried out by a state with the intention of destabilizing another state or an international organization must be considered an act of intervention in the domestic affairs of another state

Likewise, the aforementioned report *Russian Active Measure Campaigns and Interference in the 2016 US Election*, prepared by the *US Senate Select Committee on Intelligence*, argued that Russia's actions during the 2016 US presidential election were part of a broad, sophisticated, and long-standing campaign of information warfare designed to sow discord in American politics and society. In fact, for the *Committee*:

> "The IRA's actions in 2016 represent only the latest installment in an increasingly brazen interference by the Kremlin on the citizens and democratic institutions of the United States" (*United States Senate*, 2020), vol. II, p. 75).

4.2. Violation of human rights

The transmission or circulation of false information is an action that is closely related to the fundamental right to freedom of information and expression in any democracy. And this is a double-edged sword. On the one hand, freedom of expression and information guarantees that individuals or institutions can freely broadcast the information they wish, with limitations in exceptional cases. On the other hand, the transmission of false information at certain levels, for example, reaching the point of a disinformation campaign, can amount to a major violation of one of the core elements of a developed society's democratic functioning. In this regard, it is worth citing the case law of the *European Court of Human Rights* (*ECtHR*), which has reaffirmed that

> "Freedom of expression [is] one of the essential foundations of a democratic society and one of the basic conditions for its progress" (*ECtHR,* 1992, *Castells v*. *Spain*, para. 42).

At the European level, for example, this freedom is part of the fundamental rules of the Union. Thus, article 2 of the *Treaty on European Union* (*TEU*) establishes that democracy is one of the fundamental values of the Union, and it is based on the existence of free and independent media, the functioning of which requires full exercise of freedom of expression and information. This freedom is in turn guaranteed by article 11 of the *Charter of Fundamental Rights of the European Union*. According to its text, freedom of expression and information includes freedom of opinion and the freedom to receive or impart information or ideas without interference by public authorities and regardless of frontiers, as well as freedom of the media and its pluralism. In addition, article 10 of the *European Convention on Human Rights* (*ECHR*), which is also part of the EU legal system, recognizes the right to freedom of expression. According to its literal wording:

> "[...] This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

However, the text of the provision clarifies that its scope does not prevent states from requiring the licensing of radio, film, or television broadcasting enterprises first. In fact, the exercise of these freedoms, which carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions, or sanctions as are prescribed by the law of the states, provided that they constitute necessary measures to protect essential values in democratic societies. Among these values, the article lists:

> "[...] national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

For these reasons, European case law, of both the *Court of Justice of the European Union* (*CJEU*) and the *ECtHR*, when interpreting and applying the aforementioned right to information and expression, has reiterated that any limitation on freedom of expression must be interpreted restrictively, and any limitation must be imposed by normative provisions (*CJEU*, 2001, *Connolly v. European Commission*, para. 42). Primarily, the fact that the *CJEU* has warned that authorities cannot silence opinions, even if they run contrary to the official view, is noteworthy for the purposes of this article (*CJEU,* 2001, *Connolly v. European Commission*, para. 43). For the *ECtHR*, even article 10 of the *ECHR*

> "[...] 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*." (*ECtHR,* 2005, *Salov v. Ukraine*, para. 103).

Regarding the aforementioned double-edged sword, the *European Parliament* has referred to the information manipulation and disinformation in its *Resolution of 9 March 2022* on foreign interference in all democratic processes of the European Union, including disinformation, which we commented upon previously. Indeed, the *Parliament* noted, on the one hand, that

> "[...] foreign interference, information manipulation and disinformation are an abuse of the fundamental freedoms of expression and information as laid down in Article 11 of the *Charter* and threaten these freedoms [...]" (*European Parliament*, 2022b, B).

And, on the other hand, it warned that

> "[...] any action against foreign interference and information manipulation must itself respect the fundamental freedoms of expression and information" (*ibid.*, C).

In the same vein, an official document of the *Office of the Representative on Freedom of the Media* of the *Organization for Security and Co-operation in Europe* (*OSCE*) has referred to the dilemma of the right to freedom of expression/fight against disinformation, for whom,

> "[...] no 'ministries of truth' should be established to verify accuracy, current and past debates point to the duty of everyone, including public authorities, to facilitate dissemination of truthful information" (*Organization for Security and Cooperation in Europe*, 2021, para. 7).

In addition to being seen in the European legal context, this same double-edged sword of false information and disinformation campaigns as opposed to the right to freedom of expression and information is reflected universally. Thus, the *Human Rights Committee*, which is the body of independent experts that monitors the implementation of the *International Covenant on Civil and Political Rights* by its member states, has pointed out that the right to freedom of expression is broad in that it covers even expressions that may be considered deeply offensive –something that the *ECtHR* had also pointed out in its case law (*Human Rights Committee*, 2011, para. 11; *TEDH,* 1976, *Handyside v. United Kingdom*, para. 49).

The same idea is found in the *Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda* of the *United Nations Special Rapporteur on Freedom of Opinion and Expression*, and other international authorities, previously mentioned; it is emphasized that:

> "[...] the human right to impart information and ideas is not limited to 'correct' statements, that the right also protects information and ideas that may shock, offend and disturb, and that prohibitions on disinformation may violate international human rights standards, while, at the same time, this does not justify the dissemination of knowingly or recklessly false statements by official or State actors" (*United Nations Special Rapporteur on Freedom of Opinion and Expression et al.*, 2017).

The research report of the *Broadband Commission*, established by the *International Telecommunication Union* (*ITU*) and the *United Nations Educational, Scientific, and Cultural Organization* (*Unesco*), also expresses a similar view about the freedom of expression and the fight against disinformation on the Internet. According to the report:

> "Under human rights law, expression of false content –like other expression– is protected, with some exceptions. For example, under the *International Covenant on Civil and Political Rights*, certain forms of hate speech, incitement to violence, and speech that threatens human life (including dangerous health disinformation) can attract legitimate restrictions for reasons such as the protection of other human rights, or for public health purposes." (*International Telecommunication Union* and *United Nations Educational, Scientific, and Cultural Organization*, 2020).

But, as this report also highlights:

> "Nevertheless, inasmuch as speech does not reach this threshold of legitimate restriction, people have a right to express ill-founded opinions and make non-factual and unsubstantiated statements" (*ibid.*).

We may summarize this point by noting that, according to international legal standards and the practice of human rights protection bodies, as evidenced by the abovementioned document of the *Office of the OSCE Representative on Freedom of the Media*, limitations to the right to freedom of expression are permissible as long as they do not jeopardize the right itself and meet certain conditions, namely:

(1) they are prescribed by law in a sufficiently clear and precise manner;

(2) they pursue a legitimate aim, such as those enumerated in paragraph 3 of article 19 of the *International Covenant on Civil and Political Rights*, namely the protection "of the rights or reputations of others" and "the protection of national security or of public order (ordre public), or of public health or morals"; and

(3) they meet "strict tests of necessity and proportionality" (*Organization for Security and Co-operation in Europe*, 2021, para. 15).

Finally, we would like to note that, recently, in the context of the conflict in Ukraine, the *UN Human Rights Council*, in a *Resolution of 4 March 2022*, in which it examined the human rights situation in Ukraine stemming from the Russian aggression, exposed that disinformation could be one tool, among others, used to violate human rights. Specifically, the *UN Human Rights Council* expressed its concern

> "[...] at the spread of disinformation, which can be designed and implemented so as to mislead and to violate and to abuse human rights, including privacy and the freedom of individuals to seek, receive and impart information" (*United Nations*. *Human Rights Council*, 2022).

4.3. Security threat

In the end, as noted previously, certain disinformation campaigns could perhaps be qualified as real threats to the security of states or international organizations, either in and of themselves or in conjunction with other elements of the so-called hybrid threats or wars. In relation to this concept of "hybrid war" so trendy today, it seems that, as stated by **Colom-Piella** (2019, pp. 7-8), it was first used informally in an academic paper from the *US Navy* in 2002 (**Nemeth**, 2002) to refer to the tactics employed by the Chechen insurgency against the Russian forces during the First Chechen War (1994–1996), and shortly thereafter in an official US military document to explain the combination of two or more conventional threats with more disruptive ones (*United States of America Department of Defense*, 2005). For the purposes of this article, we could therefore summarize this concept, in the words of a *European External Action Service* document, as the combination of conventional and non-conventional military and non-military activities that can be employed by both state and non-state actors to achieve specific policy objectives. Among these activities, cyberattacks on critical information systems, undermining public trust in public institutions, and deepening social divisions are specifically noted in that document (*European External Action Service*, 2018). Naturally, as Colom Piella has also shown, most of these threats are not new in international society, nor are the tactics, techniques, and procedures they employ to achieve their objectives. What is new in the 21st century is the harmfulness of these threats, which comes from the exploitation of technology to maximize the informational impact in the new setting of cyberspace (**Colom-Piella**, 2019, p. 14).

Moving on to the implementation in international society to determine whether international organizations and states have considered disinformation campaigns to be threats to international security, we see that there is no shortage of official documents stating this.

Other international actors include, for example, *NATO*. In fact, the *June 2021 Brussels Summit Communiqué*, issued by the heads of state and government participating in the *North Atlantic Council* meeting in Brussels on June 14, 2021, stated that the *Alliance* is determined to employ its full range of capabilities at all times

> "[...] to actively deter, defend against, and counter the full spectrum of cyber threats, including those conducted as part of hybrid campaigns, in accordance with international law." (*North Atlantic Treaty Organization*, 2021, para. 32).

Along with this, the aforementioned document adds that the allies reaffirmed that a decision as to whether a cyberattack could lead to the invocation of article 5 of the *Treaty* should be made by the *North Atlantic Council* on a case-by-case basis, and that the impact of cumulative malicious cyber activities may, in certain circumstances, be considered tantamount to an armed attack (*ibid.*). The statement is relevant for the purposes that concern us in this article because, although it is not argued that disinformation campaigns can in certain circumstances be viewed as cyberattacks, it is not ruled out either.

Moreover, a few months later, in the *NATO Strategic Concept* adopted by the heads of state and government at the Madrid Summit of June 29, 2022, it was argued that certain authoritarian actors seek to jeopardize the interests, values, and democratic way of life of the allies, as well as undermine multilateral norms and institutions and promote authoritarian models of governance, using disinformation campaigns and other hybrid tactics. In the words of the aforementioned *NATO* instrument, referring to these authoritarian actors:

> "They interfere in our democratic processes and institutions and target the security of our citizens through hybrid tactics, both directly and through proxies. They conduct malicious activities in cyberspace and space, promote disinformation campaigns, instrumentalise migration, manipulate energy supplies and employ economic coercion. [...]" (*North Atlantic Treaty Organization*, 2022, para. 7).

The *European Parliament* has also taken the leap of considering certain disinformation campaigns to be security threats in its *Resolution of 9 March 2022* on foreign interference in all democratic processes in the European Union, including disinformation, pointing, as we know, directly to Russia and China, among others. Indeed, the *European Parliament* considered the aforementioned acts of information manipulation and other tactics of interference in democratic processes in the EU to be part of a "hybrid war strategy" and, among other things, the European Parliament ended by pointing out that they

> "[...] constitute a serious threat to EU security and sovereignty" (*European Parliament*, 2022b).

The *Council of the European Union*, for its part, has also made the connection between disinformation campaigns and jeopardizing security. Thus, the important security tool called the *Strategic Compass for Security and Defense* clearly demonstrates that Russia is threatening European order when it comes to the security and the safety of European citizens, not only through armed aggression but also through the use of "information manipulation campaigns" (*Council of the European Union*, 2022, p. 7).

In parallel to international organizations, states have considered disinformation campaigns to be threats to their security. Russia itself, in a document entitled "Russian Federation Armed Forces' Information Space Activities Concept," published on the website of the *Ministry of*

> "The impact of cumulative malicious cyber activities may, in certain circumstances, be considered tantamount to an armed attack"

Defense of the Russian Federation, recognizes that the rapid development of computer systems and electronic mass media in the third millennium has led to the creation of "a new global information space," going so far as to point out that:

> "Along with the land, sea, air and outer space, the information space has been extensively used for a wide range of military tasks in the armies of the most developed countries" (*Ministry of Defense* of the Russian Federation).

As we can see, the Russian *Ministry of Defense* considers the actions carried out in the new global information space to be one more military activity of the most developed countries. Said document even argues that, owing to the fact that information and communications systems are vulnerable to radio-electronic, software, and hardware strikes –once upon a time novel but now increasingly ubiquitous– information weapons have cross-border effects. Thus, the document concludes that:

> "[...] The role of the information warfare has sharply increased" (*ibid.*).

Similarly, *Spain's 2021 National Security Strategy* warns bluntly that

> "Disinformation campaigns have a clear impact on national security", though it does not single out Russia specifically, of course (*Government of Spain*, 2021).

The *UK's 2022 National Cyber Strategy* also deems disinformation campaigns to be a threat to national security, in conjunction with other forms of cyberattacks, also not referencing Russia specifically. In fact, according to this *British Government* document:

> "[...] Cyber attacks against the UK are conducted by an expanding range of state actors, criminal groups (sometimes acting at the direction of states or with their implicit approval) and activists for the purpose of espionage, commercial gain, sabotage and disinformation [...]" (*United Kingdom Government*, 2022, p. 9).

We will limit ourselves to citing one more example in this same line, which has been pursued by other states, as it is particularly important due to the military and geopolitical significance of the writer. We refer to the *US National Security Strategy* of October 2022, which states 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." (*United States of America*, 2022, pp. 17-18).

5. The question of reparations

As is well known from the rules of the legal system of international responsibility of states for internationally wrongful acts, from the moment a state commits an internationally wrongful act, a new legal relationship arises –the relationship of international responsibility– which results in the genesis of new obligations, in particular, the obligation to make reparations for the harmful effects arising from that act (article 28 of the 2001 *ILC draft*).

Let us recall that the first two obligations imposed on states responsible for having carried out an internationally wrongful act are the cessation and non-repetition of the wrongful conduct (article 30 of the 2001 *ILC draft*). Thus, first, the "cessation" of conduct that goes against the international obligation is the first step that must be taken by any state responsible for an internationally wrongful act, assuming that it is continuing. Second, and if the circumstances so require, the responsible state must provide

> "appropriate assurances and guarantees that it will not engage in such unlawful conduct again".

Examples of guarantees of non-repetition include the adoption of preventive measures by the offending state to avoid a new violation or a public and formal declaration by the responsible state that such acts will not be repeated in the future.

Furthermore, as we have already noted, in addition to these two obligations of cessation and of providing guarantees of non-repetition, the state responsible for having committed an internationally wrongful act must seek to eliminate all the consequences generated by that act and to restore the situation that would have existed had it not been committed. To this end, it must comply with this new and successive obligation to make full reparation for the harm caused, taking into account that such harm includes any damage, both material and moral, resulting from the wrongful conduct (article 31 of the 2001 *ILC Draft*). There are three main forms of reparation for the harm caused: restitution, compensation, and apology (article 34 of the 2001 *ILC Draft*). All of them, alone or in combination, enable the offending state to comply with the obligation to make full reparation for the harm caused.

After this brief theoretical introduction to the legal system of liability in terms of the obligation to make reparation, we should note that, in the context that concerns us in this article –that of disinformation campaigns or the dissemination of false news– the recognition of falsehood and its rectification, as forms of restitution and satisfaction, have been put forward as a possible form of reparation, under articles 35 and 37 of the 2001 *ILC draft articles* (**Baade**, 2018, p. 1369). In addition, we believe that a correct way to make reparations could be to compensate economically for the damage caused by disinformation campaigns, in parallel to or as a substitute for campaigns to rectify false information; of course, such reparation would be linked to some form of voluntary acknowledgment of responsibility or to a determination of responsibility through some means of peaceful settlement of international disputes. However, for the time being, there are no known cases in which an international dispute arising from a disinformation campaign has been submitted to any of these means of peaceful settlement, whether judicial or non-judicial.

> We have focused on Russia because it has become apparent not only to specialized researchers but to all citizens through the mainstream media that Russia has used disinformation campaigns to cloak its invasion of Ukraine in a smoke cloud of lies and half-truths

Regarding the scope of the jurisdiction of the *International Court of Justice*, we must proceed by saying that states have not yet accused each other of having used disinformation campaigns as a possible way of violating of an international obligation before it; one of these means of peaceful settlement, it is particularly interesting for our purposes because it is the principal judicial body of the *UN* and because of its track record of contributing to the determination and interpretation of international law. As no accusations have been made, no international responsibility has been attributed either. In fact, disinformation campaigns have rarely been referred to in the case law of the *Court*, except in some documents provided by the parties in support of their arguments, but in a very collateral way. One of these rare occasions was the case of *Ahmadou Sadio Diallo* (*Republic of Guinea v. Democratic Republic of Congo*) in which Guinea, in exercising diplomatic protection of one of its nationals, accused the Congo of violating the human rights of Mr. Sadio Diallo by the manner in which he was arrested, imprisoned, and then expelled, and by the manner in which his property was endangered. But Guinea did not reproach the Congo for using the weapon of disinformation. On the contrary, it was the defendant, the Democratic Republic of Congo, who invoked it, to provide proof that Mr. Sadio Diallo had been imprisoned for having carried out, among other things, disinformation campaigns against authorities or pre-eminent figures of the Democratic Republic of Congo and of other states (*International Court of Justice*, 2007b, p. 593, para. 19).

Indeed, a case of enormous interest from international practice in which one state accused another, namely Russia, of using disinformation campaigns against its interests and then held it internationally accountable is that of the Russian intervention in the 2016 US elections, already discussed in other sections.

In fact, as we have already seen, in the report *Russian Active Measure Campaigns and Interference in the 2016 U.S. Election* prepared by the *U.S. Senate Select Committee on Intelligence* to investigate Russian intervention in the 2016 US elections, purported evidence was presented that Russia had, along with other forms of cyberattacks, used disinformation campaigns on the networks to alter the results of the 2016 American elections. In fact, according to the results of the investigation of the *US Senate Select Committee on Intelligence*, certain senior officials of the *US Government* were aware of Russian attempts to intervene in the 2016 elections before they were held. A few weeks before the elections took place in November 2016, President Obama's administration even warned Moscow on several occasions; however, its response did not go further for several reasons: the fear that the reaction of the Democratic administration might appear partisan; not provoking other Russian actions; or the limited response options available at the time (*United States Senate*, 2020, vol. III, p. 159). It appears that warnings to Moscow were made at various levels, but on one occasion, President Obama himself reproached Russian President Vladimir Putin in person for such Russian interventions during the *G20* summit in Hangzhou, People's Republic of China, on September 5, 2016 (*United States Senate*, 2020, vol. III, p. 181). In the aftermath of the November 2016 elections, the Obama administration now decided to take action against Moscow in response to its interference in the elections, for example, by proceeding with sanctions against Russian individuals or companies, the expulsion of Russian government personnel, and the closure of certain Russian diplomatic properties on US territory (*ibid.*, pp. 181, 194-195).

We must conclude our discussion of this matter of practice by noting that Russia has never acknowledged its responsibility for the acts alleged by the United States and that, for the time being, the United States has not raised the issue to the level of peacefully settling international disputes, beyond the few talks or negotiations that may have taken place in this regard. As seen, the United States, in its conviction that Russia had interfered in its 2016 elections, and thus committed an international wrongdoing, resorted to self-defense, that is, countermeasures, by expelling Russian diplomats from its territory.

Another possible example of a demand for international responsibility in the scope of disinformation campaigns that Russia carried out is certain cyberattacks and the use of disinformation against democracy in the EU. On September 24, 2021, the *EU High Representative for Foreign Affairs and Security Policy*, in his *Declaration* on behalf of the European Union about the respect of democratic processes in the EU (mentioned previously) pointed to the Russian State as the party responsible for the malicious computer activities collectively called "ghostwriting"; then, he stated that the EU and its member states strongly denounced these malicious computer activities, and required that all parties involved put an immediate end to them. Finally, he announced that the EU

> "[...] will return to this issue at future meetings and will consider the possibility of adopting additional measures" (*Council of the European Union*, 2021).

As shown, here we can see a scenario of a relationship of international responsibility under the regime outlined in the *ILC* draft articles, in which we find an accusation of wrongful acts, a request for cessation of the wrongful acts, and, perhaps in the future, the demand for some other form of reparation.

We end this section by pointing out that the EU have already adopted real sanctions against Russia after the invasion of Ukraine for the use of disinformation campaigns, namely, as the President of the *European Commission* warned:

> "[...] in another unprecedented step, we will ban in the EU the Kremlin's media machine. The state-owned *Russia Today* and *Sputnik*, as well as their subsidiaries will no longer be able to spread their lies to justify Putin's war and to sow division in our Union. So we are developing tools to ban their toxic and harmful disinformation in Europe" (*European Commission*, 2022).

6. Conclusions

In this paper, we have chosen to study Russia's international responsibility for having carried out disinformation campaigns; our purpose has been to assess the importance and progress that the use of disinformation campaigns have obtained in contemporary international society as a geopolitical weapon, much like other well-established means, such as the use of force.

Following the legal system's basic rules regarding the international responsibility of parties in international society – today technically codified, among other instruments, in the 2001 *ILC draft articles on International Responsibility of States for Internationally Wrongful Acts*– we had to investigate whether the accusations against Russia were, first, that they were the perpetrator outright or behind the curtain of certain disinformation campaigns. Second, we continued by examining of these accusations or attributions of responsibility, which also has enabled us to find out what type of international obligations or norms were alleged to have been violated by Russia in using these campaigns. Third, if the conjunction of both these elements, subjective and objective, is found, this analysis would allow us to be able to affirm that a given party has committed an international wrongful act, and thus to study the cases that involve the genesis of a new legal relationship –the relationship of international responsibility, in which new legal obligations arise, such as the cessation of the violation, the obligation to provide guarantees of non-repetition, and finally the obligation to make reparations for the damage caused, through appropriate material restitution, when possible, or by means of economic compensation and/or apology.

We have focused on Russia because it has become apparent not only to specialized researchers but to all citizens through the mainstream media that Russia has used disinformation campaigns to cloak its invasion of Ukraine in a smoke cloud of lies and half-truths. This would ensure an example in which we could assess the reaction that the other actors and parties of international society had to disinformation campaigns, from those that do not cause too much verifiable damage to the victim society to those that are accompanied by hostile actions or the blatant use of armed force, which, by their very nature, are more likely to cause significant damage to the affected society.

We have seen throughout these pages how accusations from states, international organizations such as the *CE* and *NATO*, and various scientific organizations and NGOs specializing in security against Russia for making use of disinformation campaigns are becoming widespread.

Together with accusations aimed directly at Russia, something that various entities have done for many years in a more or less thinly veiled manner, in recent years we have seen how other international actors have been accusing Russia, with increasing specificity, of violating certain international norms or obligations, such as the prohibition of interfering in domestic affairs; certain human rights, such as freedom of expression and information; and the prohibition of threats to the security of states or international organizations. In particular, the United States and the EU have accused Russia of having interfered in the 2016 US election and other EU member states' elections, violating the prohibition of interfering in the domestic affairs of states and, along with it, the fundamental rights of expression and information of US and European citizens. Following the invasion of Ukraine, these accusations have been joined by others linked to this conflict, such as that of the *UN Human Rights Council*, which, in the *Resolution of 4 March 2022*, accused Russia of violating certain human rights such as the right to privacy and the freedom of individuals to seek, receive, and impart information. In addition, both *NATO* and the *CE*, through various institutions and bodies, have accused Russia of threatening their security and that of their member states by carrying out disinformation campaigns.

Finally, we are beginning to find cases in which international responsibility has been attributed to the Russian state, as in the case of Russian interference in the 2016 US elections or Russian interference in the elections of certain European states, or the use of disinformation campaigns to cover up the invasion of Ukraine. And in some of these cases, the parties who are victims of disinformation campaigns or, in the case of the invasion of Ukraine, the international parties helping it to exercise its legitimate defense, have even sanctioned the Russian state already. The US administration has sanctioned Russia in this way, for example, by expelling Russian diplomats after its interference in the 2016 US elections, and the EU has banned *Kremlin*-friendly media outlets, as announced by the President of the *European Commission*, Ursula von der Leyen, after the 2022 invasion of Ukraine.

> "Scientific entities or NGOs specialized in security or other related matters are usually reluctant to make formal accusations against Russia, even if they have found solid evidence to indicate it, most probably to avoid retaliation or allegations against them from the Russian state or the perpetrators or agents involved in these disinformation campaigns"

Thus, we find that, in the case of the Russian disinformation campaigns, the full circle of the accountability relationship has been completed. The Russian state has been accused of or blamed for carrying out these disinformation campaigns. The violation of certain international obligations has been shown, and it has been held accountable or even sanctioned for this. We have been able to verify that, in contrast, scientific entities or NGOs specialized in security or other related matters are usually reluctant to make formal accusations against Russia, even if they have found solid evidence to indicate it, most probably to avoid retaliation or allegations against them from the Russian state or the perpetrators or agents involved in these disinformation campaigns.

In light of these findings, it can be concluded that disinformation campaigns have gained significant importance as a tool of geopolitics or international relations, either on their own or in conjunction with other more classic weapons in international society, such as the age-old use of force or, effectively the same, war. In addition, I believe that this article can contribute to tipping the balance in the doctrinal debate (mentioned in the introduction) between those who think that disinformation campaigns do not greatly influence international relations and those who, on the contrary, assert that they do. In addition, because it was not the subject of this article, we could not address the question of whether disinformation campaigns contribute to modifying what the population thinks individually or collectively, which is another aspect of this debate among experts regarding the scope of disinformation campaigns; however, we believe that, indirectly, our article also proves the "usefulness" of these tools or "weapons" since, in my opinion, if states already place so much importance on disinformation campaigns, and even demand international responsibility when they are used, then these types of campaigns must have a great deal of influence on what their nationals may think.

7. References

7.1. Official documents, legislation, and case law

Centro Criptológico Nacional, Ministerio de Defensa (2019). *Desinformación en el ciberespacio*, CCN-CERT, BP/13.
https://www.dsn.gob.es/sites/dsn/files/CCN-CERT_BP_13_Desinformaci%C3%B3n%20en%20el%20Ciberespacio.pdf

Comisión de Derecho Internacional (2001). *Anuario de la Comisión de Derecho Internacional. Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53° período de sesiones*. A/CN.4/SER.A/2001/Add.1 (Part 2).
https://legal.un.org/ilc/publications/yearbooks/spanish/ilc_2001_v2_p2.pdf

Comisión Europea (2022). *Statement by President von der Leyen on further measures to respond to the Russian invasion of Ukraine*, Brussels, 27 February.
https://ec.europa.eu/commission/presscorner/detail/en/statement_22_1441

Comisión Europea y Alto Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad (2020). *Comunicación conjunta al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La lucha contra la desinformación acerca de la COVID-19: contrastando los datos, JOIN(2020) 8 final*, Bruselas, 10 de junio.

Consejo de la Unión Europea (2021). *Declaración del alto representante, en nombre de la Unión Europea, sobre el respeto de los procesos democráticos de la UE*. Comunicado de prensa, 24 de septiembre.
https://www.consilium.europa.eu/es/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes

Consejo de la Unión Europea (2022). *Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales*, aprobado por el Consejo de la Unión Europea el 21 de marzo.
https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf

Consejo Europeo (2015). *Conclusiones de la Reunión del 19 y 20 de marzo de 2015, Documento EUCO 11/15 CO EUR 1 CONCL 1*, Bruselas, 20 de marzo.
https://www.consilium.europa.eu/media/21872/st00011es15.pdf

Corte Internacional de Justicia (1986). *Military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America). Merits*, Judgment. I.C.J. Reports 1986, p. 14.

Corte Internacional de Justicia (2007a). *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007, p. 43.

Corte Internacional de Justicia (2007b). *Ahmadou Sadio Diallo (République de Guinée c. République démocratique du Congo), exceptions préliminaires, arrêt*, C.I.J. Recueil 2007, p. 582.

Gobierno de España (2021). "Real decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021", Presidencia del Gobierno. *BOE* n. 314, de 31 de diciembre.

Human Rights Committee (2011). *General Comment No 34*, CCPR/C/GC/34, 12 September.

Ministry of Defence of the Russian Federation. *Russian Federation Armed Forces' Information Space Activities Concept*.
https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

North Atlantic Treaty Organization (2021). *Brussels Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels*, 14 June.
https://www.nato.int/cps/en/natohq/news_185000.htm#32

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

Organización de las Naciones Unidas. Asamblea General (1965). *Resolución A/2131(XX), Declaración sobre la inadmisibilidad de la intervención en los asuntos internos de los Estados y protección de su independencia y soberanía.* 21 de diciembre.

Organización de las Naciones Unidas. Asamblea General (2002). *Resolución A/56/589, Responsabilidad del Estado por hechos internacionalmente ilícitos.* Distribución general 28 de enero.

Organización de las Naciones Unidas. Consejo de Derechos Humanos (2022). *Resolución 49/1. Situación de los derechos humanos en Ucrania a raíz de la agresión rusa.* Resolución aprobada por el Consejo de Derechos Humanos el 4 de marzo de 2022. A/HRC/RES/49/1.

Organización Mundial de la Salud (2018). World Health Organization. *Managing epidemics: key facts about major deadly diseases*.
https://www.who.int/emergencies/diseases/managing-epidemics-interactive.pdf

Organización para la Cooperación y el Desarrollo Económicos (2022). *Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses*.
https://www.oecd-ilibrary.org/docserver/37186bde-en.pdf

Organización para la Seguridad y la Cooperación en Europa (2021). *International law and policy on disinformation in the context of freedom of the media*. Brief paper for the Expert Meeting organized by the Office of the OSCE Representative on Freedom of the Media on 14 May.
https://www.osce.org/files/f/documents/8/a/485606.pdf

Parlamento Europeo (2022a). *Informe de la Comisión Especial sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación* (A9-0022/2022), 8 de febrero.

Parlamento Europeo (2022b). *Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación* [2020/2268(INI)].
https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_ES.pdf

Servicio Europeo de Acción Exterior (2021). *EEAS Special report update: Short assessment of narratives and disinformation around the COVID-19 pandemic* (Update December 2020 - April 2021).
https://euvsdisinfo.eu/uploads/2021/04/EEAS-Special-Report-Covid-19-vaccine-related-disinformation-6.pdf

Servicio Europeo de Acción Exterior (2022). Delegation of the European Union to Bosnia and Herzegovina & European Union Special Representative in Bosnia and Herzegovina. *Joint Statement by Ambassadors of European Union and United States to Bosnia and Herzegovina*. 6 June.
https://www.eeas.europa.eu/delegations/bosnia-and-herzegovina/joint-statement-ambassadors-european-union-and-united-states_en

TEDH (1976). Sentencia de 7 de diciembre, *Handyside c. Reino Unido*.

TEDH (1992). Sentencia de 23 de abril, *Castells c. España*.

TEDH (2005). Judgment of 6 September, *Salov v. Ukraine.*

TJUE (2001). Sentencia del Tribunal de Justicia de 6 de marzo, *Bernard Connolly c Comisión Europea.*

Unión Internacional de Telecomunicaciones (UIT) y Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2020). Balancing act: Countering digital disinformation while respecting freedom of expression. Broadband Commission research report on 'Freedom of Expression and Addressing Disinformation on the Internet'.
https://www.broadbandcommission.org/wp-content/uploads/2021/02/WGFoEDisinfo_Report2020.pdf

United Kingdom Government (2021). *National Cyber Strategy 2022*. Published 15 December.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1085304/National_Cyber_Strategy_2022_-_GOV.UK.pdf

United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information (2017), "Joint declaration on freedom of expression and fake news, disinformation and propaganda".
https://www.osce.org/files/f/documents/6/8/302796.pdf

United States of America Department of Defense (2005). *National Defense Strategy of the United States of America*. Washington DC: Government Printing Office.

United States of America Senate (2017). U.S. Senate Select Committee on Intelligence. Sarts, Janis, *The Impact of Russian Interference on Germany's 2017 Elections, Testimony before the U.S. Senate Select Committee on Intelligence*, 28 June. *http://www.intelligence.senate.gov/sites/default/files/documents/sfr-jsarts-062817b.pdf*

United States of America (2022). *National Security Strategy*, October. *https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf*

United States of America Senate (2020). U.S. Senate Select Committee on Intelligence, *Russian active measure campaigns and interference in the 2016 U.S. Election*. *https://www.intelligence.senate.gov/sites/default/files/publications/CRPT-116srpt290.pdf*

United States Senate Select Committee on Intelligence (2017). *Prepared Statement of Janis Sarts, Director of NATO Strategic Communications Centre of Excellence on Russian Interference in European Elections*. United States Senate Select Committee on Intelligence June 28. *https://www.intelligence.senate.gov/sites/default/files/documents/sfr-jsarts-062817b.pdf*

7.2. Bibliographic references

Alaphilippe, Alexandre; **Machado, Gary**; **Miguel, Raquel**; **Poldi, Francesco**; *Qurium* (2022). "Doppelganger. Media clones serving Russian propaganda". *EU DisinfoLab in partnership with Qurium*. *https://www.disinfo.eu/doppelganger*

Altheide, David L. (2004). "The control narrative of the internet. *Symbolic interaction*, v. 27, n. 2, pp. 223-245. *https://doi.org/10.1525/si.2004.27.2.223*

Baade, Björnstjern (2018). "Fake news and International Law". *European journal of international law*, v. 29, n. 4, pp. 1357-1376. *http://www.ejil.org/article.php?article=2924&issue=146*

Bernal-Hernández, Pilar (2021). "La pandemia de la desinformación". En: Blanco Souto, Miguel (coord.); Torres Jiménez, Pilar (trans.). *Riesgos pandémicos y seguridad nacional*, Granada: Editorial Universidad de Granada, pp. 93-104. ISBN: 978 84 33868374

Colom-Piella, Guillem (2019). "La amenaza híbrida: mitos, leyendas y realidades". *Documento de opinión del Instituto Español de Estudios Estratégicos*, 24/2019. *https://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO24_2019GUICOL-hibrida.pdf*

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

Corral-Hernández, David (2022). "Medios de comunicación en la guerra de Ucrania, voces y certeza frente al silencio y la desinformación". *Documento de opinión del Instituto Español de Estudios Estratégicos*, 47/2022. *https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO47_2022.pdf*

Dawson, Andrew; **Innes, Martin** (2019). "How Russia's Internet Research Agency built its disinformation campaign". *The political quarterly*, v. 90, n. 2, pp. 245-256. *https://doi.org/10.1111/1467-923X.12690*

Delcker, Janosch (2021). "Alemania: desinformación y noticias falsas asedian la campaña electoral". *DW*, 7 de septiembre. *https://www.dw.com/es/alemania-desinformaci%C3%B3n-y-noticias-falsas-asedian-la-campa%C3%B1a-electoral/a-59113186*

Egelhofer, Jana-Laura; **Lecheler, Sophie** (2019). "Fake news as a two-dimensional phenomenon: a framework and research agenda". *Annals of the International Communication Association*, v. 43, n. 2, pp. 97-116. *https://doi.org/10.1080/23808985.2019.1602782*

Espaliú-Berdud, Carlos (2022). "Legal and criminal prosecution of disinformation in Spain in the context of the European Union". *Profesional de la información*, v. 31, n. 3. *https://doi.org/10.3145/epi.2022.may.22*

Hetland, Per (2012). "Internet between utopia and dystopia, the narratives of control. *Nordicom review*, v. 33, n. 2, pp. 3-15. *https://doi.org/10.2478/nor-2013-0010*

Iosifidis, Petros; **Nicoli, Nicholas** (2020). "The battle to end fake news: A qualitative content analysis of Facebook announcements on how it combats disinformation". *The international communication gazette*, v. 82, n. 1, pp. 60-81.
https://doi.org/10.1177/1748048519880729

Lahmann, Henning (2022). "Infecting the mind: Establishing responsibility for transboundary disinformation". *European journal of international law*, v. 33, n. 2, pp. 411-440.
https://doi.org/10.1093/ejil/chac023

Lanoszka, Alexander (2019). **"**Disinformation in international politics". *European journal of international security*, n. 4, pp. 227-248.
https://doi.org/10.1017/eis.2019.6

Lasswell, Harold-Dwight (1927). *Propaganda technique in the World War*. New York: Knopf.

Marlin, Randal (2014). "Jacques Ellul and the nature of propaganda in the media". In: *The handbook of media and mass communication theory*. Robert S. Fortner; P. Mark Fackler (eds.). John Wiley & Sons, Inc., pp. 190-209. ISBN: 978 0 470675052

Messing, Solomon; **Westwood, Sean J.** (2012). "Selective exposure in the age of social media: Endorsements Trump partisan source affiliation when selecting news online". *Communication research*, v. 41, n. 8.
https://doi.org/10.1177/0093650212466406

Montes, Julio (2022). "La desinformación: un arma moderna en tiempos de guerra". *Cuadernos de periodistas*, n. 44, pp. 41-48.
https://www.cuadernosdeperiodistas.com/la-desinformacion-un-arma-moderna-en-tiempos-de-guerra

Nemeth, William J. (2002). "Future war and Chechnya: a case for hybrid warfare". Thesis, Submitted in partial fulfillment of the requirements for the degree of Master of Arts in National Security Affairs from the Naval Postgraduate School, June.
https://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf

Pizarroso-Quintero, Alejandro (1999). "La historia de la propaganda: una aproximación metodológica". *Historia y comunicación social*, n. 4, pp. 145-171.

Olmo-y-Romero, Julia-Alicia (2019). "Desinformación: concepto y perspectivas". *Real Instituto Elcano*, ARI 41/2019.
http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari41-2019-olmoromero-desinformacion-concepto-y-perspectivas

Rodríguez-Pérez, Carlos (2019). "No diga fake news, di desinformación: una revisión sobre el fenómeno de las noticias falsas y sus implicaciones". *Comunicación*, n. 40, pp. 65-74.
https://doi.org/10.18566/comunica.n40.a05

Schmitt, Michael N. (2013), *Tallinn manual on the international law applicable to cyber warfare.* Cambridge: Cambridge University Press. ISBN: 978 1 107 02443 4

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

Suárez-Serrano, Chema (2020). "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, pp. 129-154.
http://www.sybil.es/documents/ARCHIVE/Vol24/6_Suarez.pdf

Valverde-Berrocoso, Jesús; **González-Fernández, Alberto**; **Acevedo-Borrega, Jesús** (2022). "Disinformation and multiliteracy: A systematic review of the literature". *Comunicar: Revista científica iberoamericana de comunicación y educación*, n. 70, pp. 97-110.
https://doi.org/10.3916/C70-2022-08

Van-Dijk, Teun A. (2006). "Discurso y manipulación: Discusión teórica y algunas aplicaciones. *Revista signos*, n. 39, n. 60, pp. 49-74.
https://doi.org/10.4067/S0718-09342006000100003

Van-Dijk, Teun A. (2010), "Discurso, conocimiento, poder y política. Hacia un análisis crítico epistémico del discurso. *Revista de investigación lingüística*, n. 13, pp. 167-215.
http://revistas.um.es/ril/article/view/114181/108121

Wardle, Claire; **Derakhshan, Hossein** (2017). *Information disorder. Toward an interdisciplinary framework for research and policymaking*. Council of Europe.
https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c