the SPANISH YEARBOOK of INTERNATIONAL LAW

From bullets to fake news: Disinformation as a weapon of mass distraction. What solutions does International Law provide?

Chema SUÁREZ SERRANO*

Abstract: Disinformation is one of the features of the hybrid wars, arguably the most frequent types of current conflicts according to relevant international organizations such as the United Nations, the European Union or NATO, which place the so-called "fake news" among the main threats to tackle. Although disinformation is not new, the current digital means have aided tremendously in the extent and depth of their impact. These tools allow the shaping of public opinion as never before, at times determining the outcome of elections, even in nations with consolidated democracies. Could a campaign of disinformation against a state be considered an interference in its internal affairs or a violation of its national sovereignty? Could such an action represent a threat to peace and security? How to face it? Conventional warfare has given way to 'information warfare', an expression openly used by most exemplary international organizations. New approaches and new rules deem necessary.

Keywords: Armed conflicts – cyberwar – hybrid conflicts – disinformation – fake news – journalism – International Law

(A) PRELIMINARY REMARKS

It is more appropriate to refer to *false messages* than *false news*, since the latter expression is contradictory itself. News, by definition, refers to a new and true event, and false news turns out to be an oxymoron hastily coined to designate the problem we are going to face in this paper. National institutions, international organizations as well as the vast majority of researchers who approach this phenomenon from different perspectives refer it under generic name of *disinformation*, despite the fact that among citizens and even in the jargon of the media[1], the term fake news has become popular. Obviously, the aim of this work is not the nominal clarification of a concept but the concept itself: the malicious rigging operations to influence citizens by spreading false messages with the intention of taking advantage or causing harm. But according to the rigour required by scientific language we need a name, so we will call it disinformation since, as has been said, it is the preferred expression among scholars, with some nuances. A report issued by the Council of Europe[2] distinguishes three types of information disorder: dis-information (information that is false and deliberately created to cause harm), mis-information (information that is false, but not created with the

Article received on 17 July 2020, accepted on 19 October 2020 and published on 31 December 2020

* Phd. In Public International Law. Journalist in Radio Television of Andalusia (Spain). Email: chemasuarez1@gmail.com.

1 *Fundéu*, 28 September 2017.

2 Council of Europe, *Information Disorder : Toward an interdisciplinary framework for research and policy making* October 2017, at 20.

 DOI: 10.17103/sybil.24.6

intention of causing harm), and mal-information (information that is based on reality, used to inflict harm on a person, organization or country). It is convenient to make this initial clarification to avoid confusion, in a timely but brief manner lest we distract from the object of this work. We must be aware that the rapid evolution of reality generally makes sterile the effort to define it at a precise moment.

We cannot either defend the originality of this paper strictly speaking, because disinformation as a practice to achieve political or military objectives is not new at all. It has existed since a very long time ago and it has tremendously improved its methods particularly from World War II, as reveals the valuable study by D.H. Levin.[3] Its basic procedure is quite simple: disinformation consist of operations (open or secret) designed to favor any of the parties by using informative manipulation that ends up modifying the position of the citizens who remain oblivious while believing they act according to their free will, because the civil population is the main object of the attacks. Nevertheless, what is truly original now is the use of these methods at large-scale with an unattainable significance only a few years ago. Only the number of disinformation cases against European Union countries attributed to Russian sources from January to October 2019 (998 cases) is more than double that for the same period in 2018 (434 cases).[4] NATO[5] admits that deception has always been part of conventional conflicts but their influence has increased exponentially to become an essential part of modern hybrid wars, with the help of the speed and intensity offered by the internet.

Another novel aspect is the consideration of this problem as a serious threat to the security of states. Contemporary governments such as Spanish[6] place disinformation and interference in political participation among the main challenges for their own security, so we could say that these manoeuvres, barely considered until recently, have gained positions among the dangers we face nowadays, and have put us on alert only since a very recent time. The reactions made by states are still taking place in a somewhat disorderly and ineffective way, both separately and jointly (within the international organizations), and frequently in a double direction. Firstly, with the implementation of rules to prevent from disinformation dissemination and at the same time by dangerously exceeding the limits that protect freedom of expression[7], and secondly by simply warning us to be vigilant[8], which is a public

---

3 D. H. Levin, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results" *International Studies Quarterly*, Volume 60, Issue 2, June 2016, at 189–202.

4 European Parliament, Resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes.

5 Topic: NATO's response to hybrid threats, 8 August 2019.

6 Law Decree 14/2019, 31 October 2019, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Documento BOE-A-2019-15790

7 GA/RES/74/157 23 January 2020.

8 J. Althius and S. Strand, *"Fake News. A Roadmap"*, NATO Strategic Communications Centre of Excellence,

recognition that we are mired in what the European Union calls a state of *information warfare*[9]. Here we have come by malicious use of citizens' confidence and modern digital tools, used to legitimize actions that threaten sovereignty, political independence, territorial integrity of states and population security[10], charges serious enough to justify the thorough study of this problem without turning a blind eye on. In other words, disinformation violates one of the elementary principles of International Law, such as the abstention from interfering in the affairs of another state, intimately linked to the one that defends the sovereign equality of all of them. Half a century ago, the UN General Assembly declared any action against its members' political independence contrary to the principles and purposes of the Organization, which are none other than global peace:

> "Armed intervention and any other form of interference or attempted threat against the personality of the state or against the political, economic or cultural elements are in violation of international law [...] Every state has the inalienable right to choose its political, economic, social or cultural system without interference in any way by any other state."[11]

Disinformation appears as a form of interference in sovereignty, weakens peaceful coexistence and the law, and raises doubts about the validity of the tools to tackle it. We should not be surprised, because crime always moves faster than law, but the magnitude achieved raises other questions: Does the spread of large-scale disinformation truly amount a threat to global peace and security? Could a disinformation campaign against a state be considered an aggression? What is the applicable law? Would it lead to the application of International Humanitarian Law? Does it mount an interference in internal affairs or an internationally wrongful act? There are no clear answers and the community of nations is understandably concerned about the ambiguous normative.[12] The effect of disinformation and its consequences for international peace and security is also included in the UN agenda, which asks states for responsibility when using these operations and calls upon the observance of International Humanitarian Law within the course of armed conflict. The UN General Assembly[13] has called on a group of experts to present conclusions within the seventy-fifth session (2020-21) and prepares concrete actions to improve the application of International Law to the use of information and communications technologies by states.[14] They are still incipient actions, future solutions for a present problem. The Internet era represents an advance on a global basis for the exercise of public liberties, however, the question often arises

---

Riga, January 2018, at 69.

9 European Parliament, *"EU strategic communication to counteract anti EU propaganda by third parties"* 23 November 2016.

10 *Ibid* par. I.

11 GA Res. 2625 (XXV), 23 October 1970.

12 M. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, at 17 (Cambridge University Press, 2013).

13 GA Res. 73/27, 11 December 2018.

14 GA Res. 73/26, 19 January 2019.

whether it also poses a threat to democracy. Some legal, political and citizen initiatives suggest we should be critical about this subject.[15] Governments, on the one hand, make plans to defend national sovereignty against disinformation, but on the other invoke fake news to delegitimize messages contrary to their interests or to diminish critical journalists. Fear grows in the vicinity of an electoral process when taking advantage of the special sensitivity of the electorate. The OSCE asks several countries, such as Spain, for a more effective regulation to prevent people from malicious hoaxes and messages during election campaigns.[16]

Do we vote freely or manipulate? A growing number of citizens around the world show their concern for the authenticity of the information they consume mainly during election time[17], one of the battlegrounds for information warfare. Seven out of ten internet users distrust of the news during the electoral period[18] and we already know that in 2022 the citizens living in the most developed countries will consume more false news than true[19]. Nevertheless, the need to keep citizens informed appears in the 2030 Agenda promoted by the United Nations to meet the 17 objectives of sustainable development, among which we find the public access to information[20]. In this point, the Spanish government has declared its particular commitment:

> "An informed society managed by transparent and open public administrations and institutions is in a position to demand from its rulers the fulfillment of the commitments acquired by them based on proven and certain facts."[21]

The balance between information and democracy is weakening while civilians` will is targeted. As a matter of fact, citizens become enemies of their own states and simultaneously victims of the information manipulation mainly disseminated on the internet, the global space that makes us feel more capable but also the diffuse place where lies spread faster than truth. Right away we will see why.

(B) FROM TARGETING THE MILITARY TO TARGETING CIVILIANS

Deception is a clear example of a tool firstly used in armed conflicts and later developed in peacetime. It has been used largely in the realm of warfare to gain military advantage by confusing the enemy, although today it appears to be more prevalent in peacetime aiming to citizens (each one of us) for political purposes, mainly to undermine our confidence in

---

15 See, as examples of these projects, Co-inform and World forum for Democracy, Strasbourg, November 2019.

16 OSCE Report Spanish General Election.10 July 2019, at 11.

17 World Forum for Democracy 2019

18 European Commission: "*Democracy and Elections*", November 2018.

19 Gartner Top Strategic Predictions for 2018 and Beyond 3 October 2017.

20 Peace, justice and strong institutions – United Nations Sustainable Development 2015.

21 Spanish Government, Action Plan to Agenda 2030, 29 June 2018, at 63-64.

democratic institutions or influencing the election outcomes. As a matter of fact, The European Union has recently expressed deep concern about the fact that evidence of interference is continuously coming to light, often with indications of foreign influence, more in the run-up to all major national and European elections, with much of this interference benefiting anti-EU, right-wing extremist and populist candidates and targeting specific minorities and vulnerable groups including migrants, LGBTI people, religious groups, people with a Roma background and Muslims, to serve the wider purpose of undermining the appeal of democratic and equal societies. [22]

Legally speaking, peacetime and warfare are two different scenarios that require different approaches, although disinformation pursues the same purposes and techniques in both of them: obtaining particular advantages (either military or political) by using false messages (targeting military or civilians). Notwithstanding deception is an unlawful practice in peacetime, while a legal mean of war. This contradictory separation may be purely theoretical these days, since contemporary hybrid wars unfold in a blurred territory making it difficult to accurately answer the question of whether we are or not at war. While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (diplomatic, military, economic, technological), while remaining below the threshold of formally declared war.[23] With these conditions, hybrid conflicts are often difficult to be labelled, as well as the situations of war and peace. But let us start from the beginning.

According to the law of armed conflicts the lie is a legal mean of war. It has been used by the combatants since ancient times to the present days (the Tallinn Manual also defends ruses legality in the virtual sphere)[24]. In the Middle Ages Sun Tzu already warned military strategists about the importance of deception as a valuable strategy to fulfill military objectives:

> "A military operation implies deception. Even if you are competent, appear to be incompetent. Even if you are effective, prove ineffective."[25]

And so, it has been done until today, according to technical possibilities each moment. Karl Von Clausewitz already knew at the beginning of the 19th century that in military campaigns it is more important to take care of the forms than the background, namely how it is done is more relevant than what is done. During the Civil War of the United States of America (1861-1865) the army observed the rules on the conduct of hostilities elaborated by the jurist Francis

---

[22] European Parliament, *supra* n. 5 (par.5).

[23] European Commission Joint Framework on countering hybrid threats a European Union response, April 2016.

[24] M. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Second Edition (Cambridge University Press, 2017) Rule 13, at 495.

[25] SUN TZU, *El arte de la guerra*. Ed. by T. Cleary, (ed. EDAF, Madrid 2008) at 21.

Lieber, who contemplated deception as a method of war[26]. The Lieber Code included the general practice of armies and influenced the incipient codification of International Humanitarian Law. From them, we find provisions related about ruses of war in the Brussels Declaration of 1874[27], as well as in the first Hague Conventions of 1899[28] and 1907[29] that declares as lawful the war tricks and the use of the necessary means to mislead the enemy. A similar provision is contained in the norms on customary law, which authorize deception and stratagems because they do not violate any rule of IHL[30], and the same in Additional Protocol 1 to the Geneva Conventions (1977) that explicitly includes the validity of false information, making the lie a recurring legal tool[31]. Cheating, simulating, misleading, manipulating information are practices that neither violate any norm of international law, nor are perfidious since they do not target the good faith of the adversary. Until the beginning of the 20th century, deception was part of a very localized campaigns aimed at confusing the enemy on the battlefield and at specific times, but from then on they have been also oriented towards citizens, when strategists appreciated the importance of public support for the success of military operations. The First World War was a milestone as the first informative event of world relevance that aroused great interest among the population and spurred the exercise of journalism. Until that moment, International Relations were a reserved scope to governments since the time necessary or the technical difficulty for the dissemination of the chronicles, together with citizens mostly illiterate, hindered the issuance of information[32] and the exercise of journalism itself; but the First World War confrontation turned the media and public opinion into international actors –and even more so since World War II– capable of influencing the outcome of armed conflicts. Since then, success in military operations depends on the management of public opinion rather than the armies work in the field. Manipulated information emerges as an effective means to achieve it[33], what definitely involves civilians into the sphere or conflicts. In fact, the European Parliament[34] refers to this process

---

26 F. Lieber, *Instructions for the Government of Armies of the United States in the Field* (Lieber Code), 24 April 1863, Arts. 15,16 and 101.

27 Project of an International Declaration concerning the Laws and Customs of War, Brussels, 27 August 1874: Art. 14. "Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country (excepting the provisions of Article 36) are considered permissible."

28 Regulations concerning the Laws and Customs of War on Land,The Hague, 29 July 1899.

29 Article 24 of The Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907.

30 International Committee of the Red Cross (2005) Customary IHL.Art. 57 Ruses of war.

31 Additional Protocol 1 to The Geneva Conventions Art.37.2 (Adopted 8 June 1977, entered into force 7 December 1978).

32 A. Pizarroso, *Periodismo de guerra*, (Ed. Síntesis, Madrid, 2007) at. 46.

33 Ch. Suarez Serrano. *Periodismo y Derecho Internacional Humanitario, un análisis para el siglo 21.* (Dykinson, Madrid, 2017) at 236.

34 European Parliament. *supra n. 10* (par. 2).

"informative war" and points out that it is a historical phenomenon as old as the war itself, although it was not generalized until the 20th century during the Cold War to henceforth become an intrinsic part of the modern hybrid wars. If the lie has served the interest of war since immemorial time using conventional media (mainly press, radio and television) internet enlarges the wave of deception and spreads it to levels never imagined, involves the citizens without their consent but with their necessary collaboration. The objective of such attacks is altering the political, economic and social balance of the attacked country without looking like a war and of course without a formal war declaration. All will deny making use of these manoeuvres, but all include deception operations and disinformation in their military instructions[35]. Warfare overflows its limits, adopts new forms and embraces us all regardless we are civilians or living peacetime, as the European Commission warns in one of its approaches to contemporary disinformation…

> "Verifiably false or misleading information" which, cumulatively, (a) "Is created, presented and disseminated for economic gain or to intentionally deceive the public"; and (b) "May cause public harm", intended as "threats to democratic political and policymaking processes as well as public goods such as the protection of EU citizens' health, the environment or security."[36]

Which could fit the definition of conventional warfare. The secular legalization of lies as a tool for making war has brought us here. Civilization advances but the 21st century has not eliminated barbarism; it has only polished it, as *Voltaire* would say.

Although the states have been refining their disinformation campaigns and defensive strategies for decades, the incorporation of the term "fake news" into the public debate has been very recent as a result of the frequent appearance in the political discourse around 2016, simultaneously during the presidential election in the United States and Europe. Firstly, in the course of the referendum campaign that ended up with the United Kingdom withdrawal from the European Union and the following electoral processes currently happening in the European countries, conditioned by the spread of disinformation and the use of bots. The constitutional referendum in Italy (2016), the presidential elections in France (2017) or the elections to the European Parliament (2019)[37] are other examples in our immediate surroundings. In Spain, this phenomenon was consolidated in the publications of the media and among public opinion after the unlawful[38] independence referendum of October 1, 2017 in Catalonia, and the subsequent Catalan regional elections of December 21[39]. Anyhow, we have incorporated the expression "fake news" into our everyday slang. It was not in vain that

---

35 International Committee of the Red Cross (2005) Customary IHL, Practice Relating to Rule 57.

36 European Commission, Code of Practice on Disinformation, May 2019.

37 D. Barrancos, "Las elecciones más hackeables de Europa" 11 *Ciber Digest. Informe mensual de ciberseguridad*, Julio 2019, at 14.

38 Constitutional Court Judgement [STC]. 114/2017 17 October 2017 Documento BOE-A-2017-12206

39 Sociedad digital en España 2018. *Informe de la Fundación Telefónica*, at. 109-110

it was a candidate for word of the year 2017 of the famous *Fundéu*[40], a position that the English version "fake news" obtained in the United Kingdom according to the *Collins Dictionary*[41], and a year earlier, 2016, it was the word "post-truth" (post-truth) according to the *Oxford Dictionaries*[42], a term adopted by the Spanish Academy (*RAE*) in 2017[43]. In all cases, these prestigious publications had observed a notable growth in the use of these words both within the population and the media, infected by the political debate and the impulse of the social networks, which act as the first facilitators of disinformation.[44]

At the same time, the main messages exchange websites began to limit the activity of groups that disseminate false information. In the leading up days to the 2019 European Parliament elections, *Facebook* came to identify and eliminate more than 500 pages or these groups. Its content would have exceeded 500 million views across Europe, with more than 6 million followers[45]. *Facebook, Google* and *Twitter* had signed a code of conduct a few months early to prevent from the dissemination of these types of messages on the Internet, also compiled by the European Union, which alerts of threats to freedom of expression:

> "As the Commission repeatedly acknowledges in the Communication, the Signatories are mindful of the fundamental right to freedom of expression and to an open Internet, and the delicate balance which any efforts to limit the spread and impact of otherwise lawful content must strike."[46]

The European Commission set out in march 2019 the Action Plan against Disinformation, which openly recognizes the existence of the *information war (*even in peacetime*)* and the risks it poses to the values supported by democracy. Spain also reacts in 2019[47], firstly in the days before the campaigns for general elections, and secondly European and municipal processes, through the Permanent Commission against Disinformation[48], with direct participation of the Presidency of the Government and the Ministries of Defence, Home office, Foreign Affairs, and Economy and Business, which reveals the importance attached to these threats against national security, followed with concern by the media[49]. There was a prominent antecedent during the presidential elections in the United States that the Republican candidate Donald Trump won in 2016, just the year which begins the *post-truth*

---

40 *Fundéu*, 19 Diciembre 2017.

41 Collins 2017 Word of the Year Shortlist

42 Oxford Word of the Year 2016.

43 Real Academia Española, Noticias RAE. 27 Noviembre 2017.

44 J. Althius and S. Strand, *supra* n. 9, at 71.

45 D. Barrancos, *supra* n.38, at 14.

46 European Commission, *supra* n. 37.

47 European Commission, Action Plan Against Disinformation. 5 December 2018.

48 Spanish Government, Informe del Plan de lucha contra la desinformación.. 15 Marzo 2019.

49 *El País*, 11 Marzo 2019.

era[50] in which we are immersed. It is a fact that the lie spreads more quickly than the truth on the internet. According to a study[51] based on the messages in *Twitter* between 2006 and 2017, false information is spread up to one hundred times more and faster than true. Nevertheless, contrary to what was thought, the paper reveals that people disseminate disinformation as fast as robots. Our push is essential so that false messages spread up to 70 per cent more likely than a true one.

The use of disinformation as a mean of war represents a fundamental feature of hybrid warfare[52], characterized by the military and civilian components which makes it difficult to accurately determine which the applicable law is, what the legal consequences are, and how to effectively face it. The principle of distinction currently refers to clearly distinguishing between peace and wartime rather than separate military or civilian objectives in the battleground. Properly identifying whether we are in war or peace has become a challenging duty. We must bear in mind that disinformation within hybrid conflicts could provoke in peacetime similar effects than war ("public harm, intended threats to democratic political and policymaking processes as well as public goods such as the protection of EU citizens' health, the environment…" following the European Commission[53]) what according to the Tallinn Manual could derive in the same legal consequences. Years ago, it was necessary to defeat an army in the battlefield, but today it can be enough just by shaping the opponent's public opinion with floods of false messages, neither mobilizing any soldier nor using the slightest form of violence.

(C) THREATS, AGGRESSIONS. TWO OPEN QUESTIONS ABOUT DISINFORMATION.

(1) A real threat?

Eight out of ten European citizens believe that so-called fake news poses a threat to democracy[54], while seven out of ten internet users distrust the truthfulness of the information published by the media during election time[55]. These data reveal the concern about "fake news" has fully reached the population, and also that we are becoming aware of the danger they mean. NATO[56] has already included false information within the hybrid threats whose deactivation places among its priorities because of its destabilizing potential. In the same

---

50 L. Hayden, "Tell me lies, tell me sweet lies" in J. Althius and S. Strand *supra* n. 9, at 7.

51 V. Soroush, R. Deb, A. Sinan, "The spread of true and false news online" (2018) in 359 *Science*, Issue 6380, at 1146-1151 [doi: 10.1126/science.aap9559].

52 European Commission, *supra* n. 37.

53 *Ibid.*

54 European Commission. Flash Eurobarometer 464 Fake News and Disinformation Online, April 2018.

55 European Commission, *supra* n. 19.

56 NATO's response to hybrid threats, 8 August 2019

way, the European Parliament[57] has warned about the threat posed by disinformation due to its negative influence on democratic processes and citizen debate, and simultaneously the United States, China or Russia[58] face it as one of the main external risks that threaten their security. In the particular case of Spain, disinformation appears as one of the main challenges we face within the Cybersecurity Strategy (2019)[59], which shows an increase in the so-called hybrid threats, designed to attack the vulnerabilities of democratic states through traditional military actions, cyber-attacks and disinformation operations. A novel aspect, previously anticipated in the National Security Strategy (2017):

> "To the traditional armed conflicts are added additional forms of aggression [...] sophisticated systems of high precision weapons combined with the functional lethality of cyber attacks and actions of influence and misinformation."[60]

The text clarifies that the disinformation campaigns are within the so-called hybrid wars, which combine military means with cyberattacks, elements of economic pressure or campaigns of influence by social networks and information manipulation. As the National Security Strategy does, the National Security Law (2015)[61] also indicates false messages as one of the threats that compromise or undermine security, which occupies a prominent place among the main challenges posed by new technologies in the processes of political participation of citizens.[62]

To what extent could we refer to disinformation as a threat legally speaking? Answering this question is a matter of utmost importance, because the statement of "threat" is essential to decide how to deal with. International Law grants the UN Security Council the faculty to determine the existence of any threat to the peace, breach of the peace or act of aggression, as stated in article 39 of the San Francisco Charter (1945). In other words, the world's peace depends on the effective location and neutralization of the threats that endanger it, being the highest executive body of the UN in charge of such an arduous duty. In fact, this is one of the most relevant provisions of the United Nations Charter, from its very beginning:

> "The purposes of the United Nations are: Maintain international peace and security, and to that end: to take effective collective measures to prevent and removal threats to peace." [63]

However, we start from a diffuse basis because there is no more precise definition of this

---

57 European Parliament, *supra* n. 5 (par. 3).

58 The Military Doctrine of the Russian Federation, 29 june 2015

59 Spanish Government, Estrategia Nacional de Ciberseguridad (2019)

60 Royal Decree 1008/2017, de 1 de diciembre 2017, Spanish National Security Strategy 2017. BOE no. 309 21 december 2017

61 Law 36/2015, 28 September 2015, of National Security (BOE no. 233, 29 September 2015).

62 "Entre los principales desafíos que las nuevas tecnologías plantean desde el punto de vista de la seguridad pública se encuentran las actividades de desinformación, las interferencias en los procesos de participación política de la ciudadanía y el espionaje." BOE 266 5 November 2019 at 121755.

63 Charter of the United Nations art. 1 (Adopted 26 June 1945, entered into force 24 October 1945)

concept in International Law, so a "threat" will be what the Security Council shall decide in each moment, and its position varies depending on a number of factors as well as the entailed actors. Threats officially proclaimed over the years have been very diverse, almost unattainable, as Gutierrez and Cervell[64] reminds us. From the persistence of an internal armed conflict, as happened during the Balkan War (1991),[65] Angola or Rwanda, the repression of the population itself causing the risk of mass exodus (Iraq 1991),[66] the involvement in acts of international terrorism (1992),[67] massive violations of International Humanitarian Law and Human Rights during an armed conflict (1993),[68] a coup government (Haiti 1994)[69] or a military deployment at the border of a neighboring state (Iraq 1994).[70] In the 21st century the Council has seen a threat to peace when a state ignores its responsibility for protecting civil population (Libya 2011),[71] illegal trafficking of small arms (2015),[72] cultivation, production, traffic and the illicit consumption of narcotic drugs (2019),[73] the terrorist activities of the so-called Islamic state (2019),[74] or the Covid 19 pandemic (2020).[75] All these situations are officially threats, and can trigger the due responses contained in the treaties. The concept of threat as a risk to peace is also the first of the Principles of International Law declared by the UN Assembly in Resolution 2625, half a century ago (italics added):

> "Every state has the duty to refrain in its international relations from the threat or use of force against the territorial integrity or political independence of any state, *or in any other manner* inconsistent with the purposes of the United Nations."[76]

Given the impact of disinformation on the political independence of states, could it amount to *any other manner* of threat contrary to the Charter's principles? European Union seems to consider so, when arguing that electoral interference in one Member state affects the EU[77] as a whole insofar as it can have an impact on the composition of the EU institutions putting global security at risk.

---

64 C. Gutíerrez and M.J. Cervell, *El Derecho Internacional en la Encrucijada* (Ed. Trotta, Madrid, 2012) at 401.

65 SC Res 713(1991) 25 September 1991

66 SC Res 688(1991), 5 April 1991

67 SC Res 731(1992), 21 January 1992, SC Res 748(1992), 31 March 1992

68 SC Res 808(1993), 22 February 1993

69 SC Res 940(1994), 31 July 1994

70 SC Res 99 (1994), 15 October 1994

71 SC Res 1973 (2011), 17 March 2011

72 SC Res 2220 (2015/, 22 May 2015

73 SC Res 2482 (2019), 19 July 2019

74 SC Res 2490 (2019), 20 September 2019

75 S/RES/2532(2020) 1 July 2020

76 GA Res 2625 (XXV), 24 October 1970

77 European Parliament, *supra* n.5.

Malicious information has always been a factual threat capable to derive in disastrous consequences, though we seldom had neither the required sensitive nor the minimum cleverness to anticipate the calamity: In the decade of 1990, The International Criminal Tribunal for the former Yugoslavia, within the so-called *Tadic case*[78], warned us how the methodical use of today's called fake news can fuel armed conflicts. The Court sentenced that President of Serbia, Slobodan Milosevic, launched systematic disinformation campaigns through the conventional media stirring up Serbs nationalist feelings with the aim of converting an apparently friendly atmosphere between Muslims, Croats and Serbs in Bosnia and Herzegovina into one of fear, distrust and mutual hostility. The ICTY links this operation (unfolded in peacetime) with the subsequent civil war and the horrible crimes tried, which shows that disinformation poses an unheeded threat to peace:

> "After the disintegration of the former Yugoslavia began, the theme of the Serb-dominated media was that if for any one reason Serbs would become a minority population . . . their whole existence could be very perilous and endangered . . . [and therefore] they had no choice but a full-scale war against everyone else…"[79]

Other examples show how false messages still touch off lurid violence, conflicts and suffering these days, such as the persecution of Rohingyas in Myanmar.[80] The fear arises in the 21st century world, when malicious messages are widespread like never before with the internet pushing. 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. Nevertheless, none of the contemporary disinformation operations has been formally classified as a threat so far.

(a) *Interference in internal affairs.*

The principle of prohibition of threats is related to non-interference in internal affairs (United Nations Charter, article 2.7). Both of them could amount serious dangers to global stability:

> "Violation of the principle of non intervention poses a threat to the independence, freedom, and normal political, economical and social development of countries […] and can pose a serious threat to the maintenance of peace." [81]

Non intervention principle was endorsed by the International Permanent Court of Justice nearly one century ago (1927) in the "Lotus" case judgment:

> "Now the first and foremost restriction imposed by international law upon a state is that-failing the existence of a permissive rule to the contrary-it may not exercise its power in any form in the territory of

---

78 International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1992. Case No. IT-94-1-T; 7 May 1997 (par. 83)

79 *Ibid* (par. 88).

80 *The Washington Post*, 8 December 2017

81 GA Res 2131(XX), 21 December 1965.

another state."[82]

It was generally established in a treaty since Montevideo Convention (1933):

"Art. 5: The fundamental rights of states are not susceptible of being affected in any manner whatsoever."

"Art. 7: No state has the right to interfere in the internal or external affairs of another."[83]

The International Court of Justice (1986) recalls that the existence of violence it is not necessary for intervention in internal affairs to occur, but methods of coercion. This means forcing a state to behave against its sovereign will in those decisions which is able to take freely,[84] such as the choice of a political, economic, social and cultural system. All of them depend on the citizens' will expressed in free elections. UN General Assembly[85] argues that states must abstain from any defamatory campaign or hostile propaganda for the purpose of intervening or interfering in the internal affairs of others, but lately there have been growing attempts to manipulate public opinion from abroad using distorted news, even when the states are under international obligation to behave just the opposite. Such practices are harmful to the promotion of peace, cooperation and friendly relations among nations, nevertheless they are frequently used for political or war purposes.[86] The European Union also argues that fake news is a form of hostile interference in elections, as a part of a broader strategy of hybrid warfare. Such interference can take a myriad of forms, including disinformation campaigns on social media to shape public opinion.[87] Furthermore, states have also a positive obligation to fight against external (or internal) interferences that could alter the rights of citizens to freedom of expression, one of the main purposes of disinformation:

"Everyone shall have the right to hold opinions without interference. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[88]

This provision is enshrined in the most relevant treaties for the protection of fundamental rights, such as the European Convention of Human Rights (1950), the International Covenant on Civil and Political Rights (1966), the American Convention of Human Rights (1969) or the European Charter of Fundamental Rights (2012) to quote some. To this end, states must provide the free participation of citizens in electoral processes, without

---

[82] The case of SS. "Lotus" PCIJ September 7th 1927, *at* 18.

[83] Convention on Rights and Duties of States Montevideo 1933, Art.4.

[84] Case Concerning Military and Paramilitary Activities in and Against Nicaragua, ICJ, judgement. 27 June 1986 (par. 205).

[85] GA Res 73/27, 11 December 2018.

[86] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/65/201, 30 July 2010 (par.7).

[87] European Parliament, *supra* n.5.

[88] International Covenant on Civil and Political Rights. December 1966, entry into force 23 march 1976, Art. 19.1 and 2.

interference of any kind, and this means not exerting any pressure on them, and ensuring that others will not do so from abroad either. Attempts to influence the will of citizens to freely elect their political representatives represent an interference in internal affairs when carried out from outside, but also a violation of the fundamental rights of the people when deployed from within. In both cases, a violation of international (and national) law is arguable.

(b) *State Responsibility*

When a disinformation wave reaches neither the necessary threshold to endanger global peace and security to be formally declared a threat nor an unlawful interference, but causes any verifiable harm to other(s), the international responsibility of the state could be invoked. This occurs when the "responsible" state breaches an international obligation, namely when an act of that state is not in conformity with what is required of it by that obligation.[89] State responsibility is a relevant norm of the law of armed conflicts[90] (where a party which violates any obligation shall be liable to pay compensation). We also find this provision in peacetime within the draft articles on Responsibility of States for Internationally Wrongful Acts, which undeniably can be extended to hybrid conflicts in the virtual sphere, according to the Tallinn Manual guidelines.[91] The European Parliament has shown similar concern upon deeming disinformation as interference in democratic processes:

> "Such interference by other states constitutes a violation of international law, even when there is no use of military force."[92]

Disinformation could engage state responsibility under international law assuming that entails a violation of the non intervention principle, what is a breach of an international obligation. But this is a theoretical approach hardly to be proved, so the choices to claim responsibility to the state are conditioned to the arduous task of previously confirm that action:

> "The indication that an activity was launched or otherwise originates from the territory or objects of the infrastructure of a state may be insufficient in itself to attribute the activity to that state. Accusations of organizing and implementing wrongful acts brought against states should be substantiated."[93]

Another difficult question is how could an election meddling be repaired, as well as the measurement of public opinion's manipulation or even an interference in electoral outcome when revealed months or years after it took place. At this point we have to remind that satisfaction may simply consist in an acknowledgement of the breach, an expression of regret,

---

89 International Law Commission, Draft articles on Responsibility of States for Internationally Wrongful Acts,(2001) Art. 2.

90 Additional Protocol 1 to the Geneva Conventions, *supra* n. 32, Art. 91.

91 M. Schmitt, *supra* n. 25, at 80.

92 European Parliament, *supra* n.5.

93 GA Res. 73/27, 11 December 2018.

a formal apology or another appropriate modality,[94] nothing that could really make a return to the past.

(2) Aggression?

As occurs with the designation of a threat, the UN Security Council is the competent body to determine what an act of aggression is, as provided in article 39 of the Charter that we have already appointed, and it shall decide what actions must be adopted to counteract it. But contrary to the concept of threat, which lacks a precise definition, the act of aggression is quite clarified, reducing the Council's interpretation. It appears in General Assembly Resolution 3314 (XXIX) 1974[95], what basically defines aggression as the state's uses of armed force in contravention to the UN Charter. This does not mean that every use of force constitutes an act of aggression (for example the legal exercise of self-defence), but the Resolution offers some examples such as military occupation, bombing or port blocking but warns us that the list is not exhaustive, asking the Security Council to determine what other situations may become aggressions in the future. Half a century later, it is still not easy to define an act of aggression in the 21st hybrid conflicts, dominated by multidisciplinary components where the use of force generally does not exist. In the criminal jurisdiction, the signatories of the Statute of the International Criminal Court needed more than ten years to reach an agreement on the legal definition to the act of aggression, which does not appear among their powers until 2010 just to copy the position that proposed three decades before by The United Nations Assembly:

> "Act of aggression means the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the United Nations."[96]

Could interference in the internal affairs of a state through informative manipulation be considered as "any other manner" inconsistent with the Charter

The use of force and physical violence remain general premises for the identification of the act of aggression, what significantly reduces the chances. But we do not rule out this possibility because today it is commonly accepted that the violence of a hostile action depends rather on its consequences than on the means. Let us consider the use of biological, chemical or radiological agents. It goes without saying that these methods involve violent actions even if they are not accompanied by force.[97] Schmitt[98] concludes that the threshold is marked by

---

94 International Law Commission, *supra* n. 90, Art.31.

95 GA Res. 3314(XXIX), 14 December 1974.

96 Amendments to the Rome Statute of the International Criminal Court on the crime of aggression, 11 june 2010.

97 C. Droege, "Get off my cloud: cyber warfare, international law, and the protection of civilians" 94 *International Review of the Red Cross (2012)* 533-578, at 557.

98 M. Schmitt, "Wired warfare: Computer network attack and jus in bello" 84 *International Review of the Red*

the degree of suffering caused to the population, so that if the effects are only temporary discomforts or a slight decrease in the quality of life, it would not be accurate speaking of an aggression, but if it causes other more serious effects such as a collapse of the economy of democratic system, the rise of unemployment, widespread anxiety among the population, fear, panic or other situations of similar gravity, they could be taken by a full-blown. Some recent episodes show us that a scenario of this nature is not unlikely, as it happened when the dissemination of false messages about the death in a traffic accident of *Ethereum* founder, one of the most valued cryptocurrencies[99] that caused millionaire losses; or the fake news about Boris Johnson's death because of Covid-19 infection, spread from a *Twitter* account and broadcasted in Pakistan media as true.[100] Could malicious information intentionally designed against the credibility of the state's institutions, the quality of democracy, or the trust of the population provoke the same consequences? This condition remains not only for its present effects but also future, because if an action involves a latent or potential danger that will foreseeably cause serious damage to protected people or places, it might be formally declared as aggression, even though conventional violence does not exist. This is the case that in 1983 a letter from an alleged American scientist appeared in a small newspaper in Delhi, India, called *Patriot*. It was titled "AIDS May Invade India, The Mysterious Disease Caused by Experiments in the US." The text recounted how an experiment to create biological weapons in a military laboratory in Maryland had gone wrong. That piece was picked up by a Soviet scientific magazine, jumped into African newspapers and spread until four years later it reached the main evening news in the United States.[101]

From time ago some scholars[102] exclude from the definition of aggression methods such as the dissemination of propaganda or psychological and even economic warfare, and it really seems difficult to refute them with the legal arguments we still have today. But the world evolves faster than the treaties and places us in front of new challenges. Hence, the European Union[103] has already warned about the indiscriminate damages that disinformation operations cause even without the use of force, but seriously affecting the democratic processes or sensitive goods to peace and stability as the protection of health, the environment or the safety of citizens, putting us back on an unclear ground between war and peacetime. The Vice-President of the European Commission and high representative for the Union's foreign policy, Josep Borrell, warned that disinformation can kill[104] alluding to false messages

Cross (2002) 365-398, at 377-378.

99 Vitalik Buterin dead?: A hoax on 4Chan crashed ethereum's price 26 June 2017.

100 UK PM Boris Johnson's death, 9 April 2020; Fake tweet Boris Johnson's death, 7 April 2020.

101 *El País*, 25 Junio 2020.

102 M. Bothe, *New Rules for Victims of Armed Conflicts. Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Ed. Martinus Nijhoff Publishers, Dordrecht. 1982), at 289.

103 European Commission, *supra* n. 37.

104 Josep Borrell, High Representative of the EU for Foreign Affairs and Security Policy, on Twitter 23 March

spreading over the internet about Covid-19 and its influence on the population's behaviour in the face of massive contagions. In the same context the UN Secretary General has also warned about the danger posed to the population by these fraudulent and uncontrolled publications.[105] There are other doubts difficult to solve, such as the cataloguing of a disinformation campaign as an attack, a weapon or use of force. These concepts belong to the field of armed conflicts, so they are theoretically out of this scope until the connection between disinformation and a military campaign is demonstrated. New conflicts sometimes exceed the ius in bello framework, making it difficult to face with current regulations. Hybrid war does not mean that hybrid law is needed. On the contrary, the law must be clearer than ever to best tackle the new types of conflicts in this slippery domain.

The notions of attack and use of force are sometimes very close, separated for narrow details. Disinformation could be difficulty labelled as use of force according to article 2.4 of the UN Charter or as an armed attack according to article 51, thus it would not be appropriate to invoke the right to self-defence. To determine whether an object can be a weapon or in which cases its use constitutes an attack, we must resort to the rules governing the conduct of hostilities. According to Additional Protocol 1 to the Geneva Conventions,[106] an attack is an act of violence against the adversary, whether offensive or defensive, within an armed conflict. Both the existence of armed conflict and the use of violence are two implicit elements in the very concept of attack, from which it turns out that if an action does not exercise violence, for instance a disinformation campaign or even a cyber-attack, will not be considered as such unless it is framed within a war operation that involves the use of force. This is the position sustained by the International Committee of the Red Cross[107] as well as the Tallinn Manual; the operations in cyberspace (including manipulated information) could become attacks providing its effects reach the same damage level as conventional warfare. When the connection between disinformation and an armed conflict is difficult to ascertain, we could rarely consider it an attack or use of force. To that end it is compulsory to thoroughly check the consequences and damages caused,[108] which seems to be quite debatable. European Union claims for a precise and legal framework to tackle hybrid threats, both at EU and international level, in order to enable a robust response,[109] because in the meanwhile the opposite powers are taking advantage by exploiting the absence of clear rules. This is the case of Russia, whose aggressive activities in the cyber domain against European countries have

2020.

105 Antonio Gutierres, UN General Secretary, on Twitter. 28 March 2020.

106 Additional Protocol 1 to the Geneva Conventions, *supra* n. 32, Art. 49.

107 ICRC Report, International humanitarian law and the challenges of contemporary armed conflicts Geneva, 31 October 2015, *at* 39–44

108 M. Schmitt, *Tallinn Manual 2.0…supra* n.25, *at* 49.

109 European Parliament, *supra* n.5.

increased amidst legal gaps and the ambiguity of the existing ones, according to the EU.[110] Are these actions issued within an armed conflict, or using conventional violence? They definitely do not, but while discussing the precise scope or the applicable law, the problem grows. The position adopted by NATO[111] seems to take precedence over the challenge posed by hybrid threats rather than the legal framework to tackle them. This is a new domain, where the North Atlantic Organization is determined to defend itself as it does on land, sea and air:

> "We announce the establishment of Counter Hybrid Support Teams, which provide tailored, targeted assistance to Allies, upon their request, in preparing for and responding to hybrid activities. We will continue to support our partners as they strengthen their resilience in the face of hybrid challenges."[112]

Nevertheless, international law opens a chance to link disinformation with a weapon. The law of armed conflicts defines weapons as the objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.[113] Following the position issued by Droege[114], it is the intrinsic nature of an object that gives the status of weapon. But objects that are not weapons in nature may also make an effective contribution to military action by virtue of their particular location, purpose or use, which means they can acquire this condition circumstantially. This reminds us that labels are not absolute, being able to go from civil to military and vice versa in a matter of minutes. The information (true or false) disseminated by the media could become a weapon, and consequently a legal object of attacks if they either help the military effort or its destruction or neutralization results in a definite advantage; but in general, we could hardly label disinformation itself as use of any kind of force.

(D) DISINFORMATION AND NON-ARMED CONFLICTS

(1) Towards a new category of non-armed conflicts

International Law distinguishes between international or non-international armed conflicts. There are the only two legal types of armed conflicts although latest episodes would suggest a first preliminary distinction between armed and *non-armed conflicts*. Disinformation campaigns obviously belong to the last group in which conventional force does not exist, although there could be significant unarmed violence. NATO has lately showed a similar interpretation, with this warning:

---

110 European Parliament, *supra* n.10.

111 NATO, Warsaw Summit Communiqué, 8-9 July 2016.

112 NATO Brussels Summit Declaration, 11-12 July 2018.

113 Additional Protocol 1 to the Geneva Conventions, *supra* n.32, Art.52.2.

114 C. Droege, *supra* no. 98, at 562.

> "The coronavirus crisis provides insight into challenges that do not typically fall under militarised (use of force) security but could nevertheless destabilise, if not cripple, whole societies [...] The distinction between peace and war are far less clear now as disinformation and cyberattacks are continuous, rolling campaigns designed to disrupt and destabilize, possibly without end. The grey zone encompasses measures that create destabilization and conflict below the threshold of overt violence, including disruptive tactics such as disinformation, psychological operations and destabilising legal processes."[115]

Non armed conflicts, although less visible, are increasingly frequent and develop on a larger scale than those using military force. They camouflage among the mass media to feign a harmless appearance which is the basis of their success, unlike the military wars that rely on noise and opulence to generate fear. Of course, unarmed conflicts have less destructive effect than those using force, but probably a similar destabilizing potential. Can the same rules be applicable to such different forms of war? The International Court of Justice, in its Advisory Opinion on the legality of the threat or use of nuclear weapons (1996) prophesied the validity of the treaties also for the threats to come, regarding the application of the Rules of International humanitarian Law to the new weaponry:

> "It cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."[116]

This advisory opinion sheds light on the current situation, unimaginable in the 1990s. But in today's world, the only reference to their international or local area seems not to be enough for the factual classification of conflicts.

As we have seen, International Humanitarian Law is applicable to disinformation operations or cyber-attacks only if they take place in the context of an armed conflict.[117] As a matter of fact, in those cases both hostile action and its response must respect the basic principles of distinction, caution, proportionality, military necessity and humanity.[118] However, there are dissonant voices proposing new rules (even new treaties) for a situation that demands clearer rules over again. We have already said that information warfare could be hardly deemed armed operations *stricto sensu*, since it goes beyond the theoretical definition stated in the Geneva Conventions. Today these new forms of warfare are purely non armed conflicts which have come to inaugurate a new category not recognized within the International Law body that still requires the essential condition of military force.

Is it appropriate to refer to cyberwar even when the very concept of war is not clearly established? There is no legal definition, although the Criminal Tribunal for the former

---

115 NATO Review, Coronavirus, invisible threats and preparing for resilience, 20 May 2020.

116 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1 I. C.J. Reports (1996), at 226, (par.86).

117 ICRC Report, IHL and the Challenges of Contemporary Armed Conflicts. Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions, Geneva, 22 November 2019.

118 ICRC Report, International Humanitarian Law and Cyber Operations during Armed Conflicts. (Position paper) 28 November 2019.

Yugoslavia offers a valuable approach to armed conflict referring to the use of force between states, or the situation that produces continued armed violence between government forces and one or more organized groups, or between these groups within the state.[119] Recognizing the legal weight of this contribution, it does not provide much more content to the conventional subdivision established decades ago in the Geneva Conventions between International or Non-International Armed Conflicts. They still are the two only legally accepted types of conflicts, both of which have the use of armed force in common. The application of the conduct of hostilities rules in the cyberwar or in any of the operations that take place on the virtual sphere is uncertain. Today, the question as to what action short of an armed attack constitutes a use of force remains not fully resolved.[120]

(2) Non armed conflicts and freedom of expression

In times of war, lying is considered a valid method while freedom of expression is not specifically protected. In peacetime, instead, it is considered one of the fundamental rights that upholds the right of citizens to freely express or receive opinions, ideas or information by any means and without restrictions. However, most international human rights instruments do not specify whether the information must be real or false. It could be said that the veracity of information is an implicit concept, it would be better if this important detail had been laid down in the treaties to better protect the right to useful information. For example, article 19 of the International Covenant on Civil and Political Rights (1966) protects "the freedom to seek, receive and impart information and ideas of all kinds" without going into further consideration about the veracity of the messages, apart from calling upon the states to provide any lawful restriction. The same occurs with the European Convention on Human Rights (1950) whose article 10 defends the "freedom to receive or communicate information or ideas without interference from public authorities" or the European Charter of Fundamental Rights (2000) which, in its article 11 says:

> "1. Everyone has the right to freedom of expression. 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.
>
> "2. The freedom and pluralism of the media shall be respected."

A malicious reading of these treaties could conclude that they protect the dissemination of messages without any further requirements, whether true or false, avoiding the public power's interference unless the life of the nation is in danger, in which cases guarantees could be suspended for all messages, both true and false. Why do the treaties not clearly defend only true information? The approach to this fundamental right in international law opens a certain degree of ambiguity. Nevertheless, some national constitutional texts did adopt this

---

119 *Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction*, International Criminal Tribunal for the Former Yugoslavia (ICTY) The Prosecutor v. Dusko Tadic, IT-94-1-A, 2 October 1995, par. 70.

120 M. Schmitt, *Tallinn Manual 2.0…supra* n. 25, at 333.

precaution, such as the Spanish Constitution (1978) whose article 20 provides the protection of citizens against false news (emphasis added): "the right to freely communicate or receive *truthful* information by any means of dissemination." One word, *truthful*, would have been enough to undo the ambiguity within international law and make it easy to fight against false news.

States' countermeasures against disinformation must be limited by the guarantees offered by international law lest collide with the privileges enjoyed by the citizens, such as the right to freedom of expression (except in time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed[121]). Institutions such as the UNESCO, UN General Assembly or the European Commission recently warn about the practice of many governments fighting disinformation disrupting people's rights.

Both the internet and information have fully implicated the civilian population in the conflicts of the 21st century. 69 per cent of European citizens prefer to get information from the Internet, and three out of four encounter false messages at least once a week. The citizens' habits to stay up to date on current affairs have changed radically in a few years, setting the stage for the spread of disinformation.[122] People like you and me are at the same time active and passive subjects, actors and victims of these non-armed conflicts. International courts have often equated the rights and obligations of so-called citizen journalists with professionals, when it comes to recognize their contribution to denounce violations of law.[123] Disinformation equates now civilians in peacetime to soldiers in the battlefield, both targeted with the clear purpose to fulfil spurious interests. Cyberwar, hybrid conflicts, disinformation operations raise doubts about their legal approach to which instruments such as the Budapest Convention (2001)[124] or the already mentioned Tallinn Manual (2017) try to respond. The so-called Budapest Convention, or Cybercrime Convention drawn up by the Council of Europe (2001) is the first international treaty to fight crime on the internet, with specific references to support freedom of expression in the digital world:

> "The right of everyone to hold opinions without interference, as well as freedom of expression, which includes the freedom to search, obtain and communicate information and ideas of all kinds, regardless of

---

121 See International Covenant on Civil and Political Rights Art. 4, (Opened for signature at New York on 19 December 1966, Entered into force 23 March 1976). *Treaty Series*, vol. 999, p. 171, and European Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 15 (Opened for signature at Rome, 4 November 1950, entered into force 3 September 1953).

122 European Commission, Tackling online disinformation. 18 September 2019.

123 Ch. Suárez Serrano. "El Fenómeno de los Periodistas Ciudadanos en los Conflictos Armados Actuales." 36 *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades (2016)* 111-130 at 121. doi: 10.12795/araucaria.2016.i36.06

124 Council of Europe, Convention on Cybercrime (Open to signature Budapest, 23 November 2001, entered into force 1 July 2004).

borders."[125]

Any state party to the International Covenant on Civil and Political Rights (1966) availing itself of the right of derogation any of the articles, shall immediately inform the other states Parties of the provisions from which it has derogated and of the reasons by which it was actuated. The restriction must be reflected in an existing law, necessary to the objective, and for legitimate purpose as defined in the Covenant. Nevertheless, UNESCO has recently denounced the lack of enthusiasm of governments when it comes to abiding by the international rules on the protection of freedom of expression (in this particular case when addressing the Covid-19 pandemic):

> 'In the urgency to address the public health crisis, more than 80 governments around the world have declared states of emergency. Most of these countries have not notified the UN, as required by the International Covenant on Civil and Political Rights, and many of the emergency measures lack "sunset" clauses'[126]

The number of countries with specific regulations in this field has increased exponentially in the very last years.[127] states theoretically respond to the urgency of the threat in the exercise of its sovereign powers, although particular selfishness is hidden with the aim to monitor the Internet users' activity, which eventually result in the erosion of freedom of expression. When the protection of legal guarantees is forgotten, civilians become victims twice. Firstly because of the manipulative effect of malicious messages; and secondly due to the rights interruptions authorized by their own governments such as freedom of expression, officially under the need to repel the attack. Surveillance or limitation of internet use, control measures over private publications and many other measures fraudulently empower governments. The UN General Assembly insists on the actions to tackle disinformation should not collide with the protection of fundamental rights because they are not opposed objectives, but rather complement and reinforce each other:

> "Condemns unequivocally measures taken by states in violation of international human rights law aiming to or that intentionally prevent or disrupt access to or the dissemination of information online and offline, aiming to undermine the work of journalists in informing the public, including measures to unduly restrict, block or take down media websites, such as denial of service attacks, and calls upon all states to cease and refrain from these measures, which cause irreparable harm to efforts at building inclusive and peaceful knowledge societies and democracies"[128]

The European Commission[129] warns of the reprehensible action of governments that combat disinformation with actions sometimes aiming to the interruption of fundamental rights than

---

125 *Ibid*, preamble.

126 UNESCO Journalism, press freedom and COVID-19 May 2020, at 11.

127 S. Bradshaw, P.N. Howard, P. N. and L. Neudert, *Government Responses to Malicious Use of Social Media* StratCom Coe, Riga, November 2018.

128 GA Res 74/157 23 January 2020.

129 European Commission, Tackling... *supra* n. 123.

to their protection, and recalls the limits that they must observe. The European Union[130] also calls on the Member states to combat these disinformation campaigns without damaging freedom of expression, because it would be as much as collaborating with their objectives to interfere with the electoral processes or weaken the democracy or the European Union institutions. Among the alerts issued continuously by International Organizations it can also be named the privacy, a fundamental condition for the enjoyment and exercise of most of the rights and freedoms contained in the European Convention on Human Rights:

> "The rule of law is a prerequisite for the protection and promotion of the exercise of human rights and pluralistic and participatory democracy. Member states must refrain from violating the right to freedom of expression and other human rights in the digital environment."[131]

Fighting disinformation requires a global approach to efficiently neutralize its effects, since the falsehood techniques evolve faster than the defence tools designed to date. The United Nations Assembly has been working on this premise for more than a decade, with the conviction that this battle has just begun:

> "As disruptive activities using information and communications technologies grow more complex and dangerous, it is obvious that no state is able to address these threats alone. Confronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among states, and between states, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective. Therefore, the international community should examine the need for cooperative actions and mechanisms."[132]

The European Union responds to waves of fake news with different programs that mainly seek unity of states members to counteract disinformation against their interest by common guidelines. As a result, several initiatives have emerged, such as the High Level Group on fake news and disinformation, the Code of Good Practice Against Disinformation, or the Action Plan to combat disinformation appear, which is based on four pillars:

> "1. Improvement of the capacity of the Union institutions to detect, analyze and expose disinformation. 2. Reinforcement of coordinated and joint responses to disinformation. 3. Mobilization of the private sector to combat disinformation. 4. Increased awareness and response capacity of society"[133].

If the ultimate goal is to avoid the effect of false messages on public opinion, it seems obvious that action must also be taken on consumers. International organizations and governments point out the low quality of journalism and the low critical awareness of citizens, as part of the problem:

> "The financial crisis and the advancement of new forms of digital media have posed significant challenges for quality journalism, which have led to a decrease in critical thinking among the public, making it more

130 European Commission, *supra* n. 37.

131 Council of Europe, Recommendation of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries, 7 March 2018.

132 A/65/201, 30 July 2010 (par.15).

133 European Commission, *supra* n. 37.

susceptible to disinformation and manipulation."[134]

Another important aspect must be taken into account. Despite record growth in late audience ratings, the survival of the media is more than ever at risk. Advertising revenue has suddenly fallen to as much as 70 percent. This shocking reduction in their income jeopardizes the ability of the media to provide independent news coverage.[135] Simultaneously to the disinformation increasement, civil society has organized itself using precisely the facility offered by the internet, principally to denounce network cuts around the world that undermine the free flow of ideas.[136] Journalists also have recently organized in different non-profit associations to check news and eliminate hoaxes, such as the International Fact-Checking Network.[137] There are hundreds of similar initiatives tracking the virtual space every minute to locate malicious messages with the aim to return the truth to the place it should never have lost. Or rather, who never occupied either in war or in peace.

(E) FINAL CONSIDERATIONS

Are we living at war or peacetime? Few convictions resist the doubts arising from this confusing world. We are living a kind of *war without rules* according to World Economic Forum[138]or information war (following the mentioned EU position), immersed in confrontations without specific norms that disbelieve the usefulness of the treaties signed very long time ago… in the analogical era. Today's world has changed faster than law but slower than challenges. When it comes to new threats arising from hybrid conflicts, it very often remains unclear what the applicable law is. The accuracy of norms in any of the operations taking place on the internet is uncertain, specifically when there is no resource to the armed force.[139] But hybrid war cannot be faced with hybrid laws at all. On the contrary, the law must be clearer than ever to successfully tackle new threats in this slippery domain.

To better confront the new challenges disinformation poses, we have already explored the usefulness of a preliminary distinction between armed and non-armed conflicts within *jus in bello* norms, as a complement to the factual classification as international or non-international conflicts since it sometimes turns out deficient as the International Criminal Court stated.[140]

---

134 European Parliament, *supra* n. 10 (par.2).

135 Council of Europe, Declaration by the Committee of Ministers of quality of journalism on the digital age, 13 February 2019.

136 Access Now is an organization to defend and extend the digital rights of users at risk around the world.

137 IFCN Code of Principles

138 World Economic Forum, The Global Risks Report 2018

139 M. Schmitt, Tallinn Manual 2.0, *supra* n.25, at 333.

140 *Prosecutor v. Thomas Lubanga, Judgment pursuant to Article 74 of the Statute*, International Criminal Court

Furthermore, the new dangers coming from hybrid conflicts outreach the legal concept of frontiers or state's authorship, which supports the need of a more accurate approach in order to give a more efficient response. This is the European Union[141] claiming in order to counteract disinformation campaigns before it is too late. Instruments such as The Tallinn Manual 2.0 (2017) lead the fighting against disinformation and cyberspace conflicts, assuming that it needs to be constantly updating. Furthermore, other significant sources, such as European Plan of Action Against Disinformation, a number of Un Assembly General Resolutions, or the Draft Articles on States Responsibility represent valuable, inspiring instruments despite it constitutes soft law not legally binding, with limited effectiveness.

Disinformation is not only a legal and authorized method since the first codification of armed conflicts norms, paradoxically it also has contributed to humanize war, the basic premise of International Humanitarian Law. Contemporary Information warfare might become a preferable method rather than conventional armed conflicts simply because it reduces damages over the civilian population and cultural or natural heritage,[142] an argument issued decades ago in the Comments to the Protocol 1 to the Geneva Conventions:

> "A ruse is not only in no way unlawful, but is not immoral either. In many cases it will allow a successful operation with less loss of life than through the simple use of force."[143]

It would not be unrealistic to think that the laws of armed conflicts will prioritize in the near future cyberwar tools over the kinetic use of force because of the apparent lower collateral effect on objects and civilians.[144] Nevertheless, some doubts appear because disinformation as a mean of war seems to be less harmful in the short term, but we should not forget its potential effects can amount to more serious consequences, comparable to conventional war. As a matter of fact, European Union[145] has actually warned about these potentially indiscriminate damages, when seriously affecting the democratic processes or sensitive goods to peace and stability as the protection of health, the environment or the safety of citizens. As long as it does not reach that significant threshold, disinformation puts us in a midterm between the obligation of the peaceful settlement of disputes and the prohibition of the use of force, and a new way to solve international conflicts neither violating these two core principles nor causing bloody harms. This is arguably the reason for its growing presence in modern hybrid conflicts. Does it pose a threat? As said before, this is the duty of the UN Security Council, but considering its practice and having known the potential consequences, a fake news operation

(ICC), 14 March 2012, (par. 539-540).

141 European Parliament, *supra* n. 5.

142 International Committee of the Red Cross, IHL and cyber operations during armed conflicts – ICRC, November 2019, at 3.

143 International Committee of the Red Cross, Commentaries 1516 and 1521 to Additional Protocol I (1987).

144 International Committee of the Red Cross, The Potential Human Cost of Cyber Operations, May 2019, at.15.

145 European Commission, *supra* n. 37.

could be formally regarded as a threat in the near future. If such recognition has not come yet it might be because behind today's disinformation operations are mainly the most powerful and technologically developed states, many of them permanently seated in the Security Council. In other words, they have the power to veto such a similar resolution. Otherwise, the factual statement of disinformation as a threat could be a matter of very short time.

How to efficiently fight disinformation? Avoiding the impact of malicious information over the population demands on the one hand clear actions of democracy enforcement. Strong democracies would less likely fall into fake news campaigns against each other. The autocracies adopting Internet censorship and spreading disinformation online to the domestic population are more probable to also attack their neighbouring democracies than neighbouring autocracies for their geopolitical interest. In addition, the lower educational level of the population, and the greater Internet coverage increase the possibility of disinformation campaigns from abroad.[146] In the meanwhile states' countermeasures basically consist of applying the same means. The ability to respond to disinformation threats by employing a sound communication strategy deems essential,[147] but we must bear that actions designed under the label of "strategic communication" are very frequently operations of propaganda, since both pursue specific and predetermined ends. The aim of modern propaganda is not only to modify ideas, but to provoke action, to make the individual cling irrationally to a process of action,[148] just the same objective disinformation pursues. On the other hand, disinformation proliferates in a general context of low journalistic quality, which demands media professionals with the appropriate knowledge and support to build contrasted truthful messages, as well as citizens with solid critical awareness. To this achievement, independent media are necessary, endorsed by the public authorities. The United Nations, the European Union or the Council of Europe[149] insist on the importance of promoting public media so that it guarantees citizens' access to quality information, and remind governments the obligation to refrain from using them for particular purposes.

146 Ming-Chiao Chang, Chun-Chih Chang, Thung-Hong Lin. "The Art of iWar: Disinformation Campaign as a Strategy of Informational Autocracy Promotion". Paper is submitted to the 116th American Political Science Association's Annual Meeting & Exhibition, September 10-13, 2020.

147 European Parliament, *supra* n. 5.

148 J. Ellul, *Propaganda: The Formation of Men's Attitudes* (Vintage Books, New York, 1973), at 25.

149 Council of Europe, Committee of Ministers, *supra* n. 136.