Fake news, (dis)information and principle of non-intervention.

Scope, limits and possible responses to cyber election interference in times of competition.

Annachiara Rotondo
Department of Political Sciences
University of Campania Luigi Vanvitelli
Caserta, Italy
annachiararotondo@gmail.com

Pierluigi Salvati
Department of Political Sciences
University of Naples Federico II
Naples, Italy
pierluigi.salvati@gmail.com

Abstract — **In the era of asymmetrical conflicts, Information and Communication Technologies (ICT) play an essential role due to their importance in the manipulation and conditioning of public opinion[1].**

Several threats are linked to the use of ICT but, in terms of inter-state strategic competition, one of the main dangers is represented by so-called "cyber election interference", i.e. cyber election meddling activities carried out by foreign States to influence the electorate of a target State through the diffusion of 'fake news' or 'alternative truths', principally via the media and social networks (Facebook, Twitter, YouTube, etc.),

The aim of this paper is to clarify whether and when this kind of interference constitutes a breach of international obligations, in particular of the principle of non-intervention in the internal affairs of a State, and also to envisage possible lawful responses under international law for States targeted by said interference.

Keywords - cyber election meddling, international law, principle of non- intervention, options for response.

[1] As pinpointed by Stephanie Bellier "*Asymmetric warfare seeks to convert the enemy's strength into weakness, and is, therefore, especially focused on manipulating information and communication […] asymmetrical strategies aim more to influence and to change minds than to conquer*"; see S. Bellier, *Unilateral and Multilateral Preventive Self-Defense*, 58 Me. L. Rev. 508 (2006), p. 509

I. INTRODUCTION

Although the interference of foreign States in the electoral processes of other States is not a new phenomenon but is historically documented[2], some recent elections and crucial referenda[3] have brought a particular feature of this phenomenon to the attention of the international community, namely so-called 'cyber election interference'[4].

This expression does not refer herein to the physical destruction of or tampering with equipment or electoral systems, or to the modification of the results through malwares aimed at causing irregular re-counting of the votes[5].

[2] See D. H. Levin, *When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results,* International Studies Quarterly, Vol. 60, Issue 2 (2016), p. 189 ff.; see also D. Corstange and N. Marinov, *Taking Sides in Other People's Elections: The Polarizing Effect of Foreign Intervention*, American Journal of Political Science, 56 (2012), p. 655 ff.

[3] Cases of alleged foreign interference have been reported in the US and France presidential elections, Dutch and German elections, as in the 2016 Brexit and Italian constitutional referenda; for an overview, see P. Baines and N. Jones, *Influence and Interference in Foreign Elections*, The RUSI Journal, 163 (2018), 12

[4] The term 'interference' and 'intervention' are used in the present paper interchangeably, without a juridical implication, unless otherwise specified. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge: Cambridge University Press, (2017) uses the term 'interference' in reference to acts which lack the requisite of coerciveness, while the term 'intervention' refers to acts that have coercive effects.

[5] On the topic, see *amplius* M. Roscini, *Cyber Operations and the Use of Force in International Law,* Oxford University Press (2014), p. 45 ff. See the Tallinn Manual 1.0 on the International Law Applicable to Warfare, Cambridge: Cambridge University Press (2013), p. 54, where the International Group of Experts «unanimously concluded that some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the Charter»; see also Tallinn Manual 2.0, supra, p. 415; *contra*, Jaqueline Van De Velde, *The Law of Cyber Interference in Elections*, (May 15, 2017), p. 29

Nor does it refer to operations of mere cyber-intelligence collection, i.e. aimed at gathering information on electoral processes which do not seem to have *per se* characteristics of unlawfulness[6].

The reference herein is rather to non-destructive phenomena with a persuasive scope, that is campaigns of (dis)information promoted by foreign States aimed at surreptitiously influencing the vote in another State through diffusion of "fake news" or "alternative truths" principally via the media and social networks (Facebook, Twitter, YouTube, etc.),

The growing number of episodes of interference in said terms against fundamental electoral processes by foreign States makes it relevant to address the question of whether these activities constitute a breach of international law, and in particular of the principle of non-intervention in the internal affairs of a State, and to envisage possible lawful responses.

II. CYBER ELECTION INTERFERENCE AND THE PRINCIPLE OF NON-INTERVENTION IN THE INTERNAL AFFAIRS OF A STATE

Cyber election meddling can be defined as a cyber operation resulting in subtle campaigns of (dis)information[7] aimed at influencing the electoral vote and its outcome through the spread of fake news with a view to affecting the political and institutional system of the target State.

In this case, foreign intervention takes the form of activities that are more or less nuanced and not always attributable, undermining the correct formation of the will of the target State in the definition of its own government apparatus, its institutional structure and, consequently, the determination of its policies. This represents a potential violation of the principle of non-intervention in the internal affairs of a State, inasmuch as the electoral process is the highest and most significant moment of expression of domestic jurisdiction.

The principle of non-intervention is a principle of general international law [8] and has been constantly affirmed in the Resolutions of the United Nations General Assembly (UNGA)[9] with particular reference to the "sovereign and inalienable right of a State freely to determine its own political […] system, to develop its international relations […] without outside intervention, interference, subversion, coercion or threat in any form whatsoever" [10], and also with specific reference to electoral processes ("the principle of […] non-interference in the internal affairs of any State should be respected in the holding of elections")[11].

However, said principle has often been linked to the (more restricted) principle of the prohibition of the use of force, leading some scholars to sustain a substantial overlapping between them, as far as to consider the former as essentially absorbed by the latter[12].

The scope of the principle of non-intervention has been further examined by the International Court of Justice (ICJ) in the judgment *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Therein, the Court clarified the notion of 'unlawful intervention', on the one hand by delimiting its extent to matters of the target State's domestic jurisdiction [13], and on the other hand by identifying the use of methods of coercion regarding these matters as its defining characteristic[14].

Therefore, in its statement, the Court identified in coercion - *«which defines, and indeed forms the very essence of prohibited intervention*» - the parameter to affirm the unlawfulness of an episode of interference. Although the ICJ has observed that said element is *ipso facto* subsistent in the case of use of force[15], however it did not intend to reduce the hypothesis of coercive intervention exclusively to the use of force, which is albeit considered paradigmatic of the phenomenon.

Nonetheless, by omitting further examples[16], the Court did not contribute either to understanding how coercion can concretize under the threshold of the use of force or

---

[6] M. N. Schmitt, "Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law, Forthcoming in Chicago Journal of International Law, (2018), p. 21; see also Tallinn Manual 2.0, supra, p. 168

[7] Van De Velde, supra, p. 8

[8] *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*), Merits, International Court of Justice (ICJ), 27 June 1986, par. 202; see also *Corfu Channel Case (United Kingdom v. Albania); Merits;* International Court of Justice (ICJ), 9 April 1949, par. 35; Declaration on Rights and Duties of States, annexed to A/RES/374 (IV), Art. 3

[9] See e.g. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty (A/RES/20/2131); Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (A/RES/25/2625); Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States (A/RES/36/103); Respect for the principles of national sovereignty and non-interference in the internal affairs of States in their electoral processes (A/RES/50/172).

[10] A/RES/36/103, supra, Art. 2(b)

[11] See A/RES/44/147 and A/RES/50/172

[12] B. Conforti, *Diritto Internazionale*, Naples (2015), p. 270

[13] *Nicaragua*, supra, para. 205: «*A prohibited intervention must […] be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely*»

[14] Ibid.: «*Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones*»

[15] Ibid.: «*The element of coercion […] 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*».

[16] The ICJ affirmed to outline only those aspects of the principle of non-intervention which were relevant to the solution of the dispute; see *Nicaragua*, supra, para. 205

whether it is necessarily constituted by a wrongful act (or the threat of a wrongful act) [17].
Therefore, the wording of *Nicaragua* does not seem to be particularly effective in identifying further hypotheses of coercive intervention falling below the threshold of Art. 2(4) of the UN Charter, as is the case with the (dis)information campaigns which, by their very nature, do not involve the use of force.

Some authors assert that coercion could be recognized not only in the exercise (or the threat) of a wrongful act such as the use of force, but also in the forced modification of the «*normal or natural or expected course of events*»[18]. This approach is absolutely relevant for a broader interpretation of the concept of coercion beyond the paradigm provided by the ICJ in *Nicaragua* as it disconnects said notion from the threat or the implementation of an unlawful act[19] by anchoring it to a 'neutral' element, i.e. the achievement of a fact which, without the foreign intervention, would not have occurred: it would be precisely the modification of the natural course of events which would make the aforementioned intervention 'coercive'.
Also the Group of Expert Editors (GEE) of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (hereinafter "Tallinn Manual 2.0") has found that a coercive act "must have the potential for compelling the target State to engage in an action that it would otherwise not take"[20], so decoupling the concept of coercion from the commission of a wrongful act and linking it to the constraint for the target State to act in a way in which it would not have otherwise acted.
Therefore, interpreting in this sense the concept of coercion, also activities aimed at influencing the determination of political choices impacting on electoral processes might result in a coercive interference and thus in a violation of the principle of non-intervention.
On this point, the Tallinn Manual 1.0 on the International Law Applicable to Warfare (hereinafter "Tallinn Manual 1.0") already clearly stated that "cases in point [i.e. coercive] are *the manipulation by cyber means of public opinion elections* [emphasis added], as when online news services are altered in favour of a particular party, false news is spread […]"[21].
This approach is undoubtedly more suitable to extend the scope of coercion beyond the silences of *Nicaragua* and is particularly relevant with reference to the cyber operations under examination. Indeed, election meddling in the terms under discussion could result in a coercive interference inasmuch «designed to deprive another State of its freedom of choice, […] to force [the] State to act in an involuntary manner or involuntarily refrain from acting in a particular way»[22].
In this case, a key element of coercion seems to be identified in the covert nature of the foreign interference. The target State would find itself, in fact, in a situation of coercion "unbeknownst to it", i.e. without knowing it was being manipulated. The unlawful intervention - consisting of influencing the sentiments of the populace with a view to determining the results of elections - would in this case materialize as constraint through induction in that the same State would be led to take fundamental choices without having determined them autonomously and freely, thus resulting in a coercive modification of the normal or natural course of events.

A different approach based on an interpretation of coercion in terms of scales and effects achieved by the foreign intervention would lead to similar, although not identical, results.
The classical doctrine has, in fact, dwelt on the "dimensions of consequentiality" which define coercion and has identified as relevant «the importance and number of values affected, the extent to which such values are affected and the number of participants whose values are so affected» [23], which Professor Watts transposed *mutatis mutandis* into the framework of cyber operations and translated into the «nature of State interests affected […], the scale of effects the operation produces in the target State, and the reach in terms of number of actors involuntarily affected […]»[24].
In case of cyber election interference, all these 'dimensions' seem to be achieved. The free and sovereign determination of the political and institutional apparatus, and consequently of national and foreign policies, appears to be a primary interest of the State which is affected by foreign meddling. Moreover, said activity may reach, through the widespread diffusion of fake news via the media and social networks, most of the electorate, influencing its orientation in a decisive way, therefore causing it to act (i.e. to vote) on the basis of false information, which results in a manipulation of its determinations. As for the outcomes of interference, the GEE of the Tallinn Manual 2.0 affirmed that the scale of effects produced cannot be limited in terms of desired results, since the violation of the principle in question does not require the intervention to be successful: therefore, also simply forcing the electoral

[17] On the point, see Jens D. Ohlin, Did Russian Cyber Interference in the 2016 Election Violate International Law?, 95 Texas Law Review (2017), p. 1589
[18] *Amplius,* Robert Nozick, *Coercion*, in S. Morgenbesser *et al.* (Eds.), *Philosophy, Science, and Method: Essays in Honor of Ernest Nagel*, St Martin's Press (1969), p. 447
[19] On the topic, see Michell Berman, *The Normative Functions of Coercion Claims*, 8 Legal Theory 45 (2002)
[20] Tallinn Manual 2.0, supra, p. 319
[21] Tallinn Manual 1.0, supra, p. 45
[22] Tallinn Manual 2.0, supra, p. 317
[23] Myres S. McDougal and Florentino P. Feliciano, *International Coercion and World Public Order: The General Principles of the Law of War*, 67 Yale L. J. (1958), p. 782
[24] S. Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, *in* Jens D. Ohlin *et. al.* (Eds.), Cyber War: Law and Ethics for Virtual Conflict, Oxford, (2015), p. 257

process may amount to a breach of the principle of non-intervention, not being necessary the successful pursuit of the objective set by the foreign State[25].
In reality, the question of the outcome of the interference remains a debatable issue. It depends on what one considers coercive an act with the potential to compel, or solely the act which effectively compels the target State to engage in a course of action that it would otherwise not undertake.

Of course, the overall approach above should not be overestimated. It is evident that not any hypothesis in which one State pushes another to act differently to how, in the absence of its intervention, it would otherwise have acted may represent coercive interference. In fact, for the purpose of the configurability of coercion it is necessary that the target State is, in fact, 'forced', i.e. it has no other choice or possibility [26] , which mostly translates into its unawareness of being manipulated, it not being sufficient or relevant that the same has consciously modified its behaviour simply because it considers it to be advantageous (or to avoid a disadvantage).
Therefore, cases of foreign influence, such as a public campaign promoted by a foreign State aimed at inducing another State to act in a determined way (e.g., to ratify a treaty) or the endorsement of a foreign leader in favour of the election of a candidate through the media [27] cannot be considered a violation of the obligation to abstain from interfering with the internal affairs of a State. In these cases, in fact, the character of coercivity is lacking. And even cyber operations aimed at influencing a State to comply with an international obligation would not constitute a violation of the principle of non-intervention inasmuch as the subject matter is not among those in which the State «is permitted to decide freely» under *Nicaragua*[28] since the international obligation externalizes *ipso iure* compliance beyond the scope of the domestic jurisdiction[29].
Consequently, it is not easy to achieve a unitary reconstruction of the regime of foreign intervention aimed at meddling in elections through the spread of fake news, but it is necessary to carry out a holistic check on a case by case basis[30].
Therefore, the interference of a foreign State in the electoral process of another State may result in different legal qualifications, depending on the activities carried out. Thus, cyber election interference resulting in propaganda, or dissemination of real news or, on the contrary, fake news, in order to influence foreign political and electoral processes, will be subject to a different regime depending on the existence and the degree of coercion.
For this reason, for example, the lawfulness of public propaganda activities promoted by a foreign State has been affirmed: publicity, in fact, excludes the element of coercion, and thus such activity - although it may represent an unfriendly act - cannot be said to be wrongful, at least with respect to the prohibition of interference, unless a different prohibition at the level of a specific rule is provided[31].

III. QUESTIONS OF ATTRIBUTION

In order to result in a breach of the duty of non-intervention, cyber election interference must be attributable to a foreign State. In fact, attribution is an indispensable element in order to consider a determined act as an internationally wrongful act, as provided for by Art. 2 of the Draft Articles on the Responsibility of the States for Internationally Wrongful Acts (ARSIWA)[32] which reads that: «There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State».
As a matter of law, the burden of attribution has to be resolved, on a case by case basis, under strict adherence to the principles provided for under Chapter II of the same ARSIWA. Therefore, cyber election interference can be attributable to a foreign State if mainly carried out by an organ of said State (Art. 4); or persons or entities exercising elements of governmental authority of said State (Art. 5); or organs placed at the disposal of

[25] Tallinn Manual 2.0, supra, p. 322; e.g. the Council of Ministers of the Organization of African Union deplored «*the attempts* [emphasis added] by some foreign interests, through the […] manipulation of the media to interfere in and influence the outcome of the elections» in Zimbabwe in 2000; see Decision on the Developments in Zimbabwe, CM/Dec544.(LXXII)
[26] The Tallinn Manual 1.0, supra, p. 43, states that «[…] it is clear that not every form of political or economic interference violate the non-intervention principle […] It is clear that not all cyber interference automatically violates the international law prohibition on intervention: interference pure and simple is not intervention».
[27] Ohlin, supra, p. 1588
[28] *Nicaragua*, supra, para. 205
[29] Tallinn Manual 2.0, supra, p. 317
[30] Ibid., p. 319: «A few Experts, however, argued that it is impossible to prejudge whether an act constitutes intervention without knowing its specific context and consequences. For them, the context and consequences of a particular act that would not normally qualify as coercive could raise it to that level».
[31] E.g. Art. 19(2)(d) of the United Nations Convention on the Law of the Sea (UNCLOS) provides that «Passage of a foreign ship shall be considered to be prejudicial to the peace, good order or security of the coastal State if in the territorial sea it engages in any of the following activities: [..] (d) any act of propaganda aimed at affecting the defense or security of the coastal State».
[32] Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries – ARSIWA (2001) Text adopted by the International Law Commission at its fifty-third session, in 2001, and submitted to the General Assembly as a part of the Commission's report covering the work of that session (A/56/10). The report, which also contains commentaries on the draft articles, appears in the Yearbook of the International Law Commission, 2001, vol. II, Part Two, as corrected.

a State by another State (art. 6); or person or group of persons acting on the instructions of, or under the direction or control of, that State in carrying out the conduct (Art. 8)[33].

A formal attribution to a State organ under Art. 4 ARSIWA would represent the most direct ascription of the alleged interference to a foreign State, as it would be possible to trace back the intervention and attribute it even if carried out *ultra vires* (i.e. beyond the responsibility assigned to said organ)[34] and even in the case of *de facto* organs. E.g. a Report released in 2017 by the U.S. Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) under the auspices of the Office of the Director of National Intelligence (ODNI) analysed the "influence campaign" allegedly conducted by Russia in order to meddle in the 2016 U.S. Presidential election, and assessed that it was approved at the highest level of the Russian government. In particular, it denounced the participation of the main Russian intelligence service (the GRU), as well as the direct involvement of President Vladimir Putin who was attributed with having ordered said campaign[35]. In this case, the U.S. intelligence agencies have clearly attributed these activities to Russia, although they did not provide evidence in order to avoid identifying their sources, this allowing the (alleged) offending State to reject charges. However, attribution to a State organ may be, in practice, complex because often such activities are carried out by foreign secret services, and so are difficult to trace, and even when they are manifestly attributable to foreign State organs, their formal ascription to the foreign government concerned in terms of international responsibility is a further step which is not always taken by the target State[36]. E.g. even though the Special Counsel Robert Mueller's Office identified Guccifer 2.0 as a Russian intelligence officer in the light of forensic determination, and indicted him for crimes related to the alleged hacking of the Democrats in 2016[37], the response by the U.S. authorities against the Russian government was limited, after some hesitations, to a mere public accusation which did not determine any consequence under the international law of responsibility.

Very often, cyber election interference is carried out by non-state actors acting «on the instructions of, or under the direction or control of» [38] a foreign power to interfere with the target State's political system. E.g. it is the case of the Internet Research Agency (IRA), a Russian company allegedly linked to Moscow accused by the U.S. of having hired hundreds of 'trolls' to post fake news and socially divisive contents on social media as Facebook, Twitter and YouTube, and share them among millions of people [39]. In cases like this, attribution to a foreign State under Art. 8 ARSIWA lends itself to further and more complex problems. Indeed, if the concepts of 'instruction', 'direction' and 'control' are broadly meant to be understood as disjunctive[40] therefore potentially broadening the scope of attribution, the degree of control required in attributing an act committed by non-state actors to a foreign State must be identified when the State in question «directed or controlled the specific operation», and «the conduct complained of was an integral part of that operation»[41]. Only in this case, it may amount to 'effective control' in the terms outlined by the ICJ in *Nicaragua*[42].

However, in most cases, neither the 'effective control' test nor the different 'overall control test'[43] developed by the International Criminal Tribunal for the former Yugoslavia (ICTY) in the case *Prosecutor v. Duško Tadić (Appeal Judgement)* – which lowered the standard of attribution – represent a sufficient solution as both of them require a level of control and evidence on non-state actors which is hard to reach and prove in relation to cyber election interference.

Moreover, in most cases, a sure attribution of cyber interferences is not possible because of pure technical

[33] Further provisions under the ARSIWA on attribution seem to be here less relevant in practice.
[34] ARSIWA, supra, Art. 7
[35] *Assessing Russian Activities and Intentions in Recent U.S. Elections*, report released by the ODNI on 6 January 2017, available at www.dni.gov
[36] E.g. President Trump has long refused to acknowledge Russia's meddling in U.S. elections; reported in www.pbs.org
[37] See also, e.g. the Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security of 7 October 2016 where the U.S. Intelligence Community affirms «to be confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations […] These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities».
[38] ARSIWA, supra, Art. 8
[39] See U.S. Special counsel indictment in the case *United States of America v. Internet Research Agency LLC et al.,* available at www.justice.gov
[40] ARSIWA, supra, Art. 8 para. 7 of Commentary.
[41] ARSIWA, supra, Art. 8 para. 3 of Commentary.
[42] *Nicaragua*, supra, paras. 86 and 115; under the 'effective control' standard elaborated therein, the ICJ required that «For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed».
[43] In the judgment *Prosecutor v. Duško Tadić (Appeal Judgement)*, 1999, para. 145, the ICTY stated that the requisite degree of control by the Yugoslavian «authorities over these armed forces required by international law for considering the armed conflict to be international was *overall control* going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations».

problems: in fact, hackers' activities as well as the effective perpetrators of foreign interventions can hardly be traced. Also, the identification of the origin of IP routings, spoofing and other cyber means, as well as possible similarities among malwares used in hacking or spreading fake news involving a determined foreign State [44], can be considered a clue but not decisive evidence in attributing a cyber operation to said State. Even if the target State is successful in linking a determined cyber operation to a foreign State-owned infrastructure, this does not allow the target State to conclude definitively either that such cyber action effectively originated from that place or that such identification can be considered more than an indication that the State of origin may be involved with the interference. This is because non-state actors, or other States interested in muddying the waters, may have acquired control over such infrastructure[45].

Therefore, using classical standards of proof may often result in the failure to attribute these kinds of operations to a specific foreign State[46]. In all these cases, i.e. when attribution is not certain in legal terms, said activities cannot amount to an internationally unlawful act, lacking one of the two essential conditions provided by Art. 2 ARSIWA.

The question seems to be often faced by target States as a matter of fact, and therefore mainly subjected to standards of reasonability, resulting in accusations of cyber meddling which respond to prevailing political purposes and do not translate into a manifest accusation to the foreign State of having committed an "international wrongful act" [47]. In these hypotheses, electoral intervention may be considered at the least to be an unfriendly act, without entailing the international responsibility of the acting State.

IV. CYBER ELECTION MEDDLING: OPTIONS FOR RESPONSE UNDER INTERNATIONAL LAW

Even though international responsibility arises simply from the commission of an internationally wrongful act by a State, if the injured State aims to seek cessation of the conduct or to obtain reparations, it has to react through mechanisms provided by international law. This is because the lack of response may have legal consequences, such as the loss of the right to invoke responsibility, as is the case in waiver or acquiescence[48].

International law offers several options for response, the choice of which is not driven by the rule of international law but which depends on the overall balance of the opportunities and purposes of the target State. Particularly, in the case of cyber election meddling the choice of response is strictly connected to the possibility of confirming the violation of the principle of non-interference and to the ability of the target State to attribute the violation to another State.

A. Waiver or acquiescence

The practice shows that often, even in the presence of strong suspicions allowing attribution, States sometimes choose not to react at all[49].

The option of non-reaction against a wrongful act configures the hypothesis of implicit waiver or acquiescence which can represent a feasible option for an injured State. This because the target State which has reached the proof of attribution of the cyber violation committed, may want not to reveal the same in order to protect its sources and intelligence means. Inactivity seems also to respond to the will of the target State to carry out the same interference activity in turn, on the basis of a *tu quoque* practice, and not contribute to forming an express prohibitive rule.

However, it is necessary to underline that the option of waiver precludes any claim for reparation, as does the option of acquiescence. Obviously, a waiver is considered effective only if given in a valid manner, thus excluding all cases in which States express a waiver under the coercion of another State, or because of the existence of a material error.

Equally, acquiescence, as pinpointed by the ICJ in the *Certain Phosphate Lands in Nauru* case, determines the loss of the State's right to invoke responsibility[50].

Consequently, if the target State opts for non-reaction, it has to consider that it is excluding every future possibility to act against the perpetrator of the violation through instruments provided by international law (doctrine of estoppel).

---

[44] E.g. the malware found on Democratic National Committee computers seem to be the same as used by hacking groups allegedly linked to Russia intelligence services, codenamed APT 28/Fancy Bear and APT 29/Cozy Bear; reported in S. Biddle, *Here Is the Public Evidence Russia Hacked the DNC – It's Not Enough*, in The Intercept, 14 December 2016.

[45] Tallinn Manual 2.0, supra, p. 91

[46] The ICJ has not developed a standard of proof for the attribution of internationally wrongful act, assessing each dispute by case-by-case approach; the lack of case-law related to cyber interference issues does not provided for useful elements to determine *ad hoc* principles.

[47] E.g. President Obama, when announcing actions against alleged Kremlin-backed cyber interference during the 2016 Presidential elections, affirmed that «these actions […] are a necessary and appropriate response to efforts to harm U.S. interests in violation of established international norms of behavior»; see Statement of the President on Actions in Response to Russian Malicious Cyber Activity and Harassment, available at www.whitehouse.gov

[48] ARSIWA, supra, p. 119

[49] E.g. in the *Stuxnet* case, Iran did not react even if the media worldwide attributed the attack to the United States.

[50] *Certain Phosphate Lands in Nauru (Nauru v. Australia),* Preliminary Objections, Judgment, I.C.J. Reports 1992, para. 32: «*The Court recognizes that, even in the absence of any applicable treaty provision, delay on the part of a claimant State may render an application inadmissible».*

B. Countermeasures

When cyber election meddling reaches the threshold of wrongfulness inasmuch as violating the principle of non-intervention in the internal affairs and being attributed to a foreign State, the target State may resort to countermeasures which are those actions constituting a breach of an international obligation - as a breach of treaty law or of customary international law - that have to be considered lawful because the State involved has been itself victim of a wrongful act.

Under cited Art. 2 lett. a) ARSIWA, any kind of activity which determines a breach of an international obligation implies the responsibility of a State when undertaken by one of the parties cited therein[51].

In these cases, the target State can react by resorting to countermeasures within the limits expressly provided by international law, i.e. the principle of proportionality and the sole aim of inducing the responsible State to desist its ongoing unlawful conduct (thus excluding other aims such as punishment).

Moreover, under Art. 52 ARSIWA, countermeasures shall be terminated as soon as the State has complied with its obligations.

However, countermeasures do not seem an often-practicable option in the context of cyber election meddling, because of the existing disconnect between the general requirements of international law in terms of attribution and the practical necessities of States targeted by cyber operations[52].

On the one hand, international law requests the respect of discipline on international responsibility which requires attribution of the wrongful act to another State in order to allow the injured State to resort to countermeasures as well as to exhort the offending State to fulfil its obligations, to notify its intent in responding to countermeasures and to negotiate[53].

On the other hand, States need to promptly respond to cyber election interference to protect their interests, economies, citizens and territories in order to avoid, or at least contain, negative consequences.

The result is that, to date, there has been no State reaction in the form of a real countermeasure against cyber violations

In addition, even when it is possible to identify the exact location where the cyber operation originated, investigative activities often require the assistance of the authorities of the State where the interference was launched [54], and this assistance is not necessarily provided[55].

Furthermore, in carrying out cyber operations, States generally use subjects who, even after investigation, frequently remain anonymous; a further circumstance which prevents the injured State from resorting to countermeasures[56].

C. Retorsions

In the context of uncertainty around the international legal status of cyber election interference, retorsions can play an important role for States which aim to respond to preserve their interests and rights without resorting to wrongful conduct.

Indeed, measures of retorsion (i.e. «"*unfriendly" conducts which are not inconsistent with any international obligation of the State engaging in it even though may be a response to an internationally wrongful act*») [57] amount to acts which may be considered wrongful only in a political and moral sense[58].

An appropriate example of retorsion in the field of cyber election meddling was the declaration of *persona non grata* made by the U.S. Department of State with regard to thirty-five Russian intelligence operatives in response to aggressive Russian cyber activities during the last U.S. presidential election [59]. In this case, since

[51] Tallinn Manual 1.0, supra, p. 31: «*Any cyber activity undertaken by the intelligence, military, internal security, customs, or other State agencies will engage State responsibility under international law if it violates an international legal obligation applicable to that State*».

[52] «*The technology inherent in cyberwarfare makes it nearly impossible to attribute the attack to a specific source or to characterize the intent behind it. Furthermore, acts of cyberwarfare occur almost simultaneously. A legal system that requires a determination of the attacker's identity and intent does not account for these features of the digital age. The current international paradigm therefore limits the options available to states, making it difficult to effectively respond without risking a violation of international law. Restraining a state's ability to respond will encourage rogue nations, terrorist organizations, and individuals to commit increasingly severe cyberattacks*», M. Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self Defense*, Boston College International & Comparative Law Review, Vol. 32 (2009), p. 452

[53] Countermeasures presuppose attribution as stated in Art. 49 ARSIWA, reading that «*An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations»* and Art. 51 ARSIWA, reading that *«Countermeasures are limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State [and...] Countermeasures must be commensurate with the injury suffered*».

[54] R. A. Clarke and R. K. Knake, *Cyberwar*, Harper Collins Publisher, New York (2010), p. 215

[55] «*Although states can trace the cyberattack back to a computer server in another state, conclusively ascertaining the identity of the attacker requires an intensive, time consuming investigation with assistance from the state of origin [...] This attribution problem locks states into the response crisis*», M. J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: a Justification for the Use of Active Defenses Against States Who Neglect their Duty to Prevent*, Military Law Review/Vol. 201 (2009), pp. 7 and 8

[56] Tallinn Manual 1.0, supra, p. 31: «States may contract with a private company to conduct States cyber operations. Similarly, States have reportedly called upon private citizens to conduct cyber operations against other States or targets abroad».

[57] ARSIWA, supra, p. 128 of Commentary.

[58] M. N. Schmitt, supra, p. 25

[59] In the past, retorsions included all forms of retaliation by a State against another in response of all kind of unwelcome acts by the latter. Nowadays, this concept is limited only to those actions which do not interfere with the target State's rights under international law; *amplius*

international law does not oblige States to maintain relations with other States, the declaration of *persona non grata* and the following expulsion of intelligence operatives constituted a mere unfriendly act.

Because of its characterization, retorsion seems to be the most practicable legal functional response in case of non-attributable cyber election interference.

The so-called 'active defence strategies', consisting of cyber-operations - including those of a preventative nature - that the target State may resort to without having previously assessed the attribution of the interference to another State, can be considered a form of retorsion[60].

Such activities can be allowed owing to the fact that these kinds of measures should never reach the threshold of unlawful conduct, as they are limited to striking the systems from which the attack has been launched in order to avoid damage within the territory of the target State[61]. Indeed, as they are focused on impeding damage by the incoming cyber-operations, they should be considered an instrument available to States to ensure the integrity of their territories and the security of their population within the exercise of their sovereign powers.

The lawfulness of retorsions depends on the relation between means and ends which, if imbalanced (e.g. when a State interrupts the supply of vital goods to another State only with the aim of exercising coercion in matters of its domestic jurisdiction), pushes the retorsion beyond the threshold of lawfulness[62].

T. Giegerich, *Retorsion*, in R. Wolfrum (Ed.), *The Max Plank Encyclopedia of Public International Law*, Oxford (2012), p. 976

[60] On the point, see M. Hoisington, supra, p. 453, according to which the international community should promulgate a list of "critical national infrastructure" whose violation via cyber-attack would authorize the State upon whose territory the infrastructure lies to respond via active defense measures without incurring in international legal responsibility but, above all, without the loss of time involved in identifying the author of the attack.

[61] «Active defense measures, however, use offensive means in order to defend against and neutralized a threat. The purpose of using a cyber counterattack is to stop a specific, immediate, or ongoing cyber threat rather retaliate with a strategic purpose. It is offensive action for a defense purpose», C. Lotrionte, *Active Defense for Cyber: A Legal Framework for Covert Countermeasures*, in J. Carr (Ed.), *Inside Cyber Warfare*, O'Reilly Media (2011), p. 274

[62] T. Giegerich, supra, p. 980

V. CONCLUSIONS

The complex and uncertain legal qualification of cyber activities resulting in electoral meddling, mostly due to their hard attribution, represents a serious concern for States struck in their electoral processes.

The last G7 Summit held in Cananda on June 2018 heavily stressed the danger posed by attempts on the part of foreign actors to weaken democratic societies and institutions by undermining their electoral preocesses through «malicious, multi-faced and evolving tactics [which] constitute a serious strategic threat»[63].

However, the same legal uncertainty can be considered an opportunity for target States which can obtain strategic advantages through cyber counter-operations, aimed at containing collateral effects without enatiling international responsibility. This perspective should not necessarily be considered negative because nothing impedes – as previously demonstrated – target States from reacting through international law mechanisms not resulting in internationally wrongful acts, more precisely retorsions, which seem to be a functional tool in terms of results.

In fact, above all if carried out in the cyber domain, retorsions are able to reach results analogous to those achievable through countermeasures which, in turn, would put the target State which wants to respond to the cyber election interference at serious risk of violating international law.

If States aim to reduce their vulnerabilities and contrast cyber threats such as cyber election meddling, strategy can not be solely based on legal responses. A further preventive effort, in terms of strenghtening cyber-defense capabilities to protect electoral processes, is a fundamental issue.

On this point, it is to be noted that some States are strengthening their electoral systems, with the cooperation of their respective intelligence organizations, with a view to avoiding foreign interference in future elections.

E.g., Australia has formed an *ad hoc* task force ("Electoral Integrity Task Force" - EITF) to guard its election process against foreign cyber interference involving multiple agencies with a particular attention on strengthening precautionary measures. Led by the Home Affairs Department and involving the Australian Security Intelligence Organisation, the Australian Federal Police, as well as the Department of Finance and the Australian Electoral Commission, the EITF aims to avoid foreign interference in elections. In addition, the government of Australia has decided to

[63] Charlevoix Commitment on Defending Democracy from Foreign Threats, G7 Summit, Charlevoix, 9 June 2018, available at www.g7.gc.ca

adopt an *ad hoc* legislation to prevent foreign electoral meddling[64].

Even the European Union (EU) has developed a strategy to counter propaganda and disinformation: in 2015, the Council of the EU tasked the High Representative for Foreign Affairs and Security Policy to submit an action plan on strategic communication[65] which led to the establishment within the EU's External Action Service of a Unit named European Strategic Communication Task Force (StratCom) to challenge foreign (mainly Russian) disinformation campaigns.
StratCom is to date divided into three units – StratCom East, South and Western Balkans – even though the main body is represented by StratCom East which is the one tasked with identifying, analysing and raising awareness about pro-Kremlin disinformation and aimed at increasing public awareness of disinformation activities by foreign powers and improving the EU's capacity to anticipate and respond to such challenges. In September 2017, a website was launched featuring a database of over 3,000 cases of disinformation as well as giving an overview of the latest fakes published and explaining how trolling and manipulation in media really work.
More recently, in January 2018, the European Commission set up a High-Level Expert Group (HLEG)[66] to contribute to the development of an EU-level strategy in facing the spread of fake news. In March 2018, the HLEG presented a report suggesting a multi-dimensional approach to the issue based on five pillars consisting of concrete and inter-dependent actions ranging from enhanced transparency to the promotion of media and information literacy to counter disinformation[67].
Despite all these efforts, the European Parliament recently newly urged the Union to increase its resilience to Russian propaganda[68].

A significant contribution to contrasting the spread of fake news aimed at influencing the electorate could also come from the most popular media and social networks, which should strengthen their internal tools for verifying the authenticity of news and profiles. Even on this point, new initiatives seem to have been undertaken[69] although the choice of the concrete tools to be used in contrasting disinformation keep raising questions under different points of view, e.g. the protection of the right to freedom of expression.

The fact is that cyber phenomena are not purely legal in nature so to fully understand and, consequently, contrast them, States have to think in terms of integrated strategies which cannot avoid the involvment of international law, but at the same time, must require the active intervention of other disciplines.

[64] reported in www.reuters.com
[65] European Council meeting (19 and 20 March 2015) – Conclusions, para. 13
[66] The HLEG consisted of 39 members coming from academia, journalism, press and broadcasting organizations, online platforms as well as civil society and fact-checking organization; see 'A multi-dimensional approach to disinformation' - Report of the independent High-level Group on fake news and online disinformation, presented on March 2018 and available at www.ec.europa.eu
[67] Ibid, p. 20
[68] reported in www.europarl.europa.eu
[69] see e.g. Mark Zuckerberg, 'Protecting democracy is an arms race. Here's how Facebook can help', 4 September 2018, reported in www.washigtonpost.com