SIOI
UNA Italy

OSSERVATORIO
sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana

Misinformation and online radicalization: a debate on the role of the UN in the context of COVID-19 "infodemic"

Antonio Perrelli
Dottorando di ricerca in "Governo dell'Impresa, dell'Amministrazione e della Società nella Dimensione Internazionale", Università degli Studi di Teramo

1. COVID-19 and radicalization: a brief introduction. A year after the declaration of Public Health Emergency of International Concern by the World Health Organization, containment strategies for COVID-19 seem to face a process of normalization, in terms of both policies and legislative tools. In spite of that, a few domains still stay, at least partially, uncovered. The aim of the present paper is to draw attention to one of those areas, namely counter-terrorism. Given the context of an augmented use of the social media, a sharp increase in online recruitment by extremist groups was indeed observed. A special focus will therefore be given to the problematic linkage between disinformation and online radicalization.

Such premises will expose a practical *causatum* for the work of the United Nations, which will be of particular interest for the case, with special regard to fallouts concerning security policies. Being the largest multilateral policy provider in the field, the UN has indeed to take over the sensible task of coping with new forms of radical proselytism, such as the ones related to misinformation. The present work will hence deepen the current scenario, as well as its historical background, in an attempt to hypothesize how policies and legislation might look like in the near future.

2. Countering terrorism under the United Nations legislative framework. In order to better observe the impact of fake news and radicalization in the context of UN legislation, one must preliminary examine how terrorism phenomena are framed, not just semantically, but with a view to countermeasures. Historically, the UN approach consists of three main phases[1], as the whole process of collective security has to be studied through a long-term angle, from the dawn of multilateralism to date. Initially, a non-coercive, multilateral and regionalized response took place, approximately going from the early years of the League of Nations to the late forties. Right after the outbreak of Cold War, we witness a similar set-up, accompanied by a smooth transition towards an executive-led paradigm (marked by a more centralized governance model). September 11 attacks moved things further, bracing the path towards a more militarized and security-based approach, with a conspicuous influence of the Security Council. Such a long journey has been wrapped up in three cornerstones of UN counter-terrorism legislation, United Nations Security Council (UNSC) Resolutions 1373 (2001), 1267 (1999), and 1624 (2005)[2]. Other significant examples of targeted soft-law instruments

[1] A.M. Salinas De Frias, K. Samuel, N. White, *Counter-Terrorism, International Law and Practice*, Oxford, 2012.

[2] C.M. Minnella, *Counter-Terrorism Resolutions and Listing of Terrorists and Their Organizations by the United Nations*, in E. Shor, S. Hoadley (eds.), *International Human Rights and Counter-Terrorism, International Human Rights*, Singapore, 2019.

on the matter include Security Council Resolutions 1540 (2004), 1673 (2005) on weapons of mass destruction, Security Council Resolutions 1333 (2000), 1390 (2002), 1735 (2006) on Al-Qaida and the Taliban, and UN Global Counter-Terrorism Strategy (2006). All of these latter constitute, alongside with sixteen conventions, protocols and amendments, the so-called Global Legal Framework against Terrorism[3]. It comes as no surprise that a definition of terrorism is deliberately nebulous through the abovementioned pieces of legislation, even if the UN Counter-Terrorism Committee (CTC) itself has conferred a precise connotation to the term. Such a clarification was exposed in the context of UNSC Resolution 1566, and has its roots in the Terrorist Financing Convention of 1999. Nevertheless, the Global Legal Framework against Terrorism remains, at least partially, vague. The ensuing open-clause of terrorism provides greater freedom for States in terms of lawmaking policies, with the sole compulsion of keeping a fairly wide field of application for the international terrorism framework[4].

Under such a scenario, it is of a certain interest to remark how the main task remains not to define what terrorism is, but what it is not. Such a peculiarity has been observed, for instance, regarding the Draft Comprehensive Convention on International Terrorism negotiations, where theoretical clashes emerged on the distinction between terrorist organizations and liberation movements. As a definition of terrorism is hence partially lacking on a multilateral level, we should consider it as comprehensive of emerging categories, whether applicable. It remains vital to keep a special focus on the risks of threat anticipation strategies, as they should not take place in the absence of *ad hoc* mechanisms monitoring the Rule of Law. The problem, constituting a major point in the field of prodromal acts of terrorism, becomes even more crucial when it comes to acts of recruitment and propaganda for the benefit of extremist groups. Eventually, it is self-evident that when all of these human activities take place on a dematerialized space as the Internet, a fair balance between the respect of the rule of law and the rightful anticipation of criminal offence is difficult to achieve.

3. Fake news: from self-standing category to emerging radicalization expression. In the light of the abovementioned *lacunae*, another epistemic problem arise: if a definition of terrorism remains strongly related to a shared perception of phenomena, is it rightful to refer to emerging categories in order to enforce counter-terrorism legal framework? As for the present case: may the spreading of fake news be considered, under certain conditions, an act of terrorism? The adverse impact of fake news on legal systems is nothing new in the field of International Law, as customary and conventional tools have regulated it through the last century. As a way of example, we can observe the norm of customary international law defining the obligation of non-intervention (Prohibition of Intervention), the 1936 International Convention on the Use of Broadcasting in the Cause of Peace and the 1953 Convention on the International

[3] UNODC, *The Universal Legal Framework against Terrorism*, Funa Futi, Tuvalu, National Workshop 24, 27, April 2009.

[4] B. Saul, *Defining Terrorism in International Law,* Oxford, 2006.

Right of Correction[5]. As for the umbrella term *terrorism*, the expression *fake news* tends to describe a wide variety of technical and common use situations. It is somehow impossible, then, to locate a generously open clause inside another one.

Whilst a semantic definition for both terms is lacking, the United Nations Interregional Crime and Justice Research Institute (UNICRI) provided a report showing a certain linkup between the two processes[6]. Emphasis is thus put on the specific goal of malicious information: in point of fact, online radicalization by the means of fake news seems to affect three main theoretical clusters, concerning right-wing extremists, Islamic State in Iraq and the Levant (ISIL or Da'esh) and Al-Qaida groups, and the organized crime. Despite the fact that the process seems to occur heterogeneously and according to regional circumstances, triggers and dissemination channels present shared features. At the same time, distorted information targets diverse subject matters depending on extremist groups: far-right movements, for instance, push for a total collapse of society, calling for an *etnostate*. This is what has been recently observed with Accelerationists, Boogaloo, white suprematists, MAGA, Qanon supporters and WASP (as reported with respect to the Capitol Hill assault in the United States). Conspiracy theories are hence tailored to the needs of the group: in the context of COVID-19 pandemic, the schemes of far-right movements hence tend to attribute the spreading of the virus to immigrants and foreigners, while ISIL and Al-Qaida (as well as Al-Shabaab) try to mark the pandemic as an ally in the fight against western countries. It is interesting to observe how terrorists from far-right groups work to delegitimize governments and plot violent attacks targeting both symbols of democracy and minorities, whilst organized crime is willing to take over a subrogate form of authority by substituting state-actors through pseudo-volunteering campaigns. The process results, most of the time, in charity programs aimed at supporting rural people and local vulnerable groups, as noticed in Italy and Mexico[7].

4. The militarization of UN counter-terrorism model: from multilateralism to security. There is no doubt that the Security Council has a vital role to play in the field of counter-terrorism. As already observed, a major shift in the benefit of the UNSC occurred as a consequence of 11 September 2001, resulting in a centralization of counter-terrorism policies[8]. Today, we wonder if such a securitization can still constitute a valid response strategy for what seems to be a decades-old emergency. Therefore, the process of counter-radicalization seems to perform better results (at least on the long distance and on a wider scale) if not violently pursued[9]. The severe impact of fake news on online radicalization hence reveals the feebleness of existing strategies, increasingly oriented to a path of militarization of counter-terrorism. First and foremost,

[5] B. Baade, *Fake News and International Law*, in *European Journal of International Law*, 2018, pp. 1357-1376.

[6] UNICRI, *Stop the Virus of Disinformation, the risk of malicious use of social media during COVID-19 and the technology options to fight it*, 2020 Edition, UNICRI: Turin.

[7] UNICRI, op. cit.

[8] B. Saul, op. cit.

[9] A opposed to the scenario conceived in A.M. Dershowitz, *Why Terrorism Works: Understanding the Threat, Responding to the Challenge*, New Haven, 2003.

the present approach unwarrantedly neglects dematerialized areas of human life, such as the interactions taking place on the Internet. Secondly, a sanction-oriented focus reduces the chances to tackle the problem in the future, marginalizing prevention policies. Counter-terrorism measures may indeed indicate a different path for the years to come, getting back to the former approach of an extended multilateralism, with a growing participation of the General Assembly.

The wish for a return to a multilateral policy making model is somehow emphasized by the vast amount of delegates calling for the problem on a regional scale, as made clear by interventions of many representatives through the first meeting of the seventy-fifth session of the Sixth Committee of General Assembly in 2020[10]. Cambodian delegate, speaking for the Association of Southeast Asian Nations ASEAN, pointed out how COVID-19 crisis exposed already susceptible individuals, increasing the risk of online radicalization. Saudi Arabia representative highlighted a process of discrimination towards Muslim minorities via fake news and mendacious online propaganda. Norway's delegate stressed the role of misinformation in the process of defamation regarding the Government (such a process can easily relate to many other western liberal democracies, as previously noted with regards to right-wing extremists)[11].

5. UN and terrorism prevention policies: how to curb the phenomenon of online radicalization by means of misinformation. Such a fragmented and unclear context, weighted down by lexical uncertainty and ideological hostilities, cannot be mend other than through counter-policies specifically aimed at preventing radicalization to occur via fake news. This does not imply that misinformation should constitute a subgroup into the wider spectrum of terrorism. To this effect, the scope is not to comprehend whether fake news fall into the unclear definition of online radicalization (and terrorism), but to raise awareness on the impact that such a policy area may have on the existing Global Legal Framework against Terrorism, as the United Nations already boasts effective soft-law tools targeting fake news and guiding Internet users to evidence-based information. The more we theoretically merge misinformation and terrorism together, the more our paradigm will embrace a security-based model. If we aim at a framework built on prevention, we should therefore pursue a two-headed approach, preserving existing categories and methods separately.

Moreover, risk scenarios exposed by the UNICRI report[12] on the matter suggest how patterns of radicalization via fake news may involve a wide variety of demagogy techniques, depending on actors and subjects involved. Such an assumption further complicates a deeply tangled scenario. A clarification is hence needed: while the narrative of organized criminal groups does not resort to mainstream media channels, far-right, ISIL, Da'esh and Al-Qaida seem to need social media and online press (even though indirectly) in order to offer the picture of a para-institutionalized crusade to at-

[10] UN General Assembly Sixth Committee, 75th Sess, 1st Plen Mtg, GA/L/3614 (6 October 2020).
[11] UNICRI, op. cit.
[12] UNICRI, op. cit.

risk individuals. The process takes place, in most cases, through the channels of private users, which remain the main spreaders of what a joint-statement of WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, and IFRC has recently defined a COVID-19 *infodemic*[13]. In addition, a document released by the UN Department of Global Communications (DGC) defined some target-subjects (identified in the early stages of COVID-19 pandemic) as the most sensible areas of potential misinformation[14]. The reflection included production and dissemination of medical information, partnerships with businesses such as social medias and telecommunication companies, supporting the work of media and journalists, mobilization of civil society and human rights safeguard measures.

Once framing methods have been clarified, one must define how to directly tackle the problem of online radicalization via fake news, shaping a model based on prevention policies. *Modi operandi* described by UNICRI in the previously discussed report allow us to articulate a prevention system based on technology. Among a wide variety of options, it is worth mentioning the potential role of data science, big data visualization, machine learning algorithms for large–scale disinformation scenarios; tools and platforms based on artificial intelligence with regards to the *ex ante* fake news detection process; mobile apps and chatbots powered by fact-checkers and web-browsers as for the general public; digital media information literacy platforms and tools in connection with the lack of consciousness of online users.

6. Conclusion. In light of the above, expanding the existing prevention policies and supporting technological advancement could prove to be an effective strategy for the UN, *in lieu* of tightening the criminal framework by encouraging unlinked regional policies and promoting *de facto* security-based counter-terrorism models. As previously described, boosting digital literacy and *ex ante* fact-checking methods (at least for social media and digital press) will certainly play a role in shaping policies and legislation in the future. Alongside with a stronger commitment from the General Assembly, there must therefore be the willingness to rebuild priorities around the underlying causes of radicalism and, as regards the present case, to structure a renovated model of prevention.

Marzo 2021

[13] Such a perspective is reported in the statement *Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation*, Joint statement by WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, and IFRC (www.who.int).

[14] In order to better understand the ongoing UN strategies facing the so called infodemic, we might refer to the document of the DGC *5 ways the UN is fighting 'infodemic' of misinformation* (www.un.org).