

DISINFORMATION BULLETIN

ISSUE 4 • 29 JUNE 2020

disinformation

A CALL TO ACTION AGAINST DISINFORMATION

BY SOPHIE KENNEALLY

AGENFOR INTERNATIONAL NEWSLETTER

AGENFORMEDIA.COM

COMMUNICATION @ AGENFORMEDIA.COM

LINKEDIN: LINKEDIN.COM/COMPAN Y/AGENFOR-MEDIA

AKE

10th June, the European On Commission published their joint addressing communication on disinformation during the COVID-19 (henceforth, crisis the Communication). The report reiterated a number of serious concerns that have been raised repeatedly following the outbreak of the virus late last year, while also bringing to light several important new recommendations. This article elicits some of the key implications and challenges raised by the latest Communication concerning diverse actors involved in countering disinformation.

The clearest message echoed throughout the Communication was that to counter disinformation, Europe must take a "whole-ofsociety" approach. Adopting this approach, first set out in the EU Action Plan Against Disinformation[1], means reinforcing the army of actors proactively engaged in tackling disinformation, ensuring it is multilevel, multi-competence, and multidisciplinary. The plurality of the different categories of disinformation demands a corresponding plurality of responses, taken by a range of actors or, better said, the whole of society. Precisely which actors should be involved and when, depends on several factors, including the topic of disinformation, the channels in which it spreads, the community targeted (international. local, vulnerable groups), and, as explicitly noted by the Commission. whether the disinformation constitutes "illegal content, as defined by law, [or] content that is harmful but not illegal".

In response to the first distinction, relating to the topic of the content, the Commission calls for clear and effective communication of verifiable information from relevant official organisations, a measure that has been emphasised repeatedly by the Commission as the coronavirus crisis unfolds. Naturally, in the case of COVID-19, this means ensuring that accurate public health advice is communicated to all members of however this society. level of communication is also essential in relation to public matters such as transport or travel guidelines, social distancing rules, or changes in social welfare and support mechanisms, as well as matters managed by private bodies, such as email servers and banks.

The second factor, concerning the media used to spread disinformation, is one that is fully inseparable from the phenomenon itself. These platforms, both on- and offline, faced hard criticism long-before the advent of the novel coronavirus (and justifiably so). They are in a key position to strengthen the

identification of fake news, its sources, and trends in its diffusion, as well as to take action to prevent and respond to it. Accordingly, the Communication reiterates the need for an "intensified role for online platforms in the crisis", referring to the EU Code of Practice on Disinformation[2], and outlining a more stringent monitoring plan. The third matter -- the target of disinformation -- is one that has thus far received little attention in counterdisinformation strategies but which is touched upon in the Communication. Understanding the community targeted by any security threat is key to its prevention, yet particularly in the cyberworld, this can be a difficult task. Determining the most relevant actors in responding to the phenomenon requires understanding the scale and an geographical spread of the target community. Where the circulation of disinformation content is confined to one country, for example, we might expect to see the involvement of predominantly national or local actors, who have a better understanding of the community and their environment, and are likely in a better position to communicate risks to them. Where, on the other hand, content diffuses beyond national borders, a coordinated response is required from competent international organisations and between national governments. While very little research has been conducted on who is more vulnerable to disinformation, and while we can say with relative certainty that the community is unexclusive, there are some factors that expose certain individuals to greater risks. Most notably, the Communication calls for particular attention to be given to "vulnerable groups, for example young people and children, who face a higher risk of being misled and as a consequence expose themselves to more dangerous situations".

^[1]https://eeas.europa.eu/sites/eeas/f iles/action_plan_against_disinformat ion.pdf.

^[2] https://ec.europa.eu/digitalsingle-market/en/news/codepractice-disinformation

This is an important consideration when deciding who should implement measures to increase resilience (teachers, parents, CSOs), in which thev environments should he (schools, implemented in the workplace, etc.), and which form they should take (media literacy courses, awareness campaigns, etc.) and is one that undoubtedly requires further research.

The final distinction that we can elicit from the Communication is perhaps the most problematic. It differentiates content that is illegal from content that is harmful, but legal. This is a critical issue common to all security risks and pivotal in determining which instruments can be used and under whose competence intervention should fall. Where disinformation content constitutes a crime according to national or EU legislation, new actors and instruments are called into play. Some such activities associated with disinformation are criminalised under existing areas of national legislation, such as consumer protection or illegal hate speech laws, while others are provided for under more broadly defined laws targeting disinformation itself. Provisions falling into the latter category have been introduced in several Member States prior to the pandemic (such as German the 2017 Netzwerkdurchsetzungsgesetz or the French Loi nº 2018-1201), and, in Hungary, as a direct response to it (Anti-Coronavirus Act[3]).

Introducing laws that define (certain) disinformation content as illegal means mobilising law enforcement agencies (LEAs) and their respective instruments. While there are significant advantages to reinforcing the counter-disinformation army with LEAs, the Communication highlights that introducing a criminal dimension to disinformation seriously risks undermining the sanctity of the freedom of expression and pluralistic democratic debate. In Europe, the potential of such laws to conflict with fundamental rights and democratic values has meant that legal responses to disinformation remain nascent and LEAs rarely involved.

Criminalising disinformation, in one way or another, also requires a typology of the phenomenon to establish whether a law has been violated. This is a complex task, not least because identifying the recognising authors and their motivations within the vast cyber space challenges even the most advanced artificial intelligence tools. Generally speaking, when talking of inaccurate information, we differentiate between misinformation and disinformation. based on the author's intent. In the case of misinformation, the content is unintentionally inaccurate (it does not reader), aim to deceive the disinformation, on the other hand, is intentionally false or misleading (designed to deceive). To this dichotomy, the Communication adds a third category: foreign influence operations, which include

"...covert actions by foreign governments intended to sow divisions in our society, undermine confidence in our democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives.[4]"

By introducing this category, we make a further shift from LEAs (concerned with criminal investigations and limited to a strict set of investigative tools) to intelligence agencies, mandated with countering foreign influence activities and employing a very different set of instruments. These two independent roles, with distinct entities, responsibilities, and modi operandi are both needed to reduce the threat of false information, however, knowing when to involve which entity, requires a distinction between clear misinformation, disinformation, and foreign influence activities (which remains highly complex), as well as the integration of these terms into legal frameworks (which remains highly contentious).

distinctions highlight the These complexity of disinformation dynamics and reaffirm the need to treat it as a serious and multifaceted security threat. The Communication is clear in expressing the paramount importance of responding to this threat with a colourful armament of instruments, from journalists' notepads, to automated fact-checking tools, social media monitoring, to media literacy campaigns. Employing these instruments calls for a deeper understanding of the phenomenon and a response from whole of society in a combined and sustained effort to counter disinformation in, and long after, the COVID-19 era.

Read the full Communication "Tackling COVID-19 disinformation -- Getting the facts right" here: https://ec.europa.eu/info/sites/info/f iles/communication-tackling-covid-19disinformation-getting-factsright_en.pdf

[3] On 16th June, Hungarian MPs voted to end the contentious emergency powers under this provision https://www.france24.com/en/2020061 6-hungary-mps-approve-end-ofcontroversial-emergency-virus-powers

[4] United States Department of Justice https://www.justice.gov/jm/jm-9-90000-national-security

FOR MORE INFORMATION ON THIS TOPIC AND ON OUR PROJECTS PLEASE VISIT AGENFORMEDIA.COM

