




COMMENTARY


Hybrid threats in times of COVID-19: how is the EU responding to the Russian-driven disinformation campaign?

VOCAL
EUROPE

*This commentary was written by **Radu-Ion Gheorghe** | 20 April 2020

 Rue de la Science 14, 1040 Brussels

 office@vocaleurope.eu

 + 32 02 588 00 14

HYBRID THREATS IN TIMES OF COVID-19: HOW IS THE EU RESPONDING TO THE RUSSIAN-DRIVEN DISINFORMATION CAMPAIGN?

VOCAL EUROPE

RUE DE LA SCIENCE 14B, 1040 BRUSSELS

TEL: +32 02 588 00 14

VOCALEUROPE.EU



[TWITTER.COM/THEVOCAL EUROPE](https://twitter.com/thevoCALEUROPE)



[FACEBOOK.COM/VOCAL EUROPE](https://facebook.com/vocaleurope)



[YOUTUBE.COM/VOCAL EUROPE](https://youtube.com/vocaleurope)



[INSTAGRAM.COM/VOCAL EUROPE](https://instagram.com/vocaleurope)

Disclaimer and Copyright

This document is prepared for, and addressed to Vocal Europe and its audience. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of Vocal Europe. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged.

HYBRID THREATS IN TIMES OF COVID-19: HOW IS THE EU RESPONDING TO THE RUSSIAN-DRIVEN DISINFORMATION CAMPAIGN?

Introduction

The COVID-19 outbreak has spread relentlessly across the globe in the past few months. It has brought unprecedented challenges to healthcare systems in almost every country in the world, but it also has other worrisome implications, including elements of hybrid warfare such as cyberattacks and disinformation. Since the crisis began, a series of fake news and misleading information about COVID-19 has been spotted circulating online, in particular on social media.

In February 2020, speaking about the spread of misinformation and disinformation related to the coronavirus pandemic, Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization (WHO) said that these types of activities are a part of an “infodemic”. He also underlined the fact that disinformation “spreads faster and more easily than this virus.”¹

The EU has accused Russia of carrying out a disinformation campaign about COVID-19 which targets citizens of EU member states and partner countries², thus having the potential to present a risk to public health and well-being of its citizens. The messages promoted through this campaign aim at showcasing Russia’s preparedness to deal with the crisis, while also undermining the EU’s efforts to tackling the spread of coronavirus.

At the same time, this alleged pro-Kremlin campaign also includes the dissemination of false or misleading information about vaccines and medicines against the virus in order to create confusion and widespread panic and to prevent people from accessing accurate information about the disease and safety provisions.³

Under these circumstances, on 3 March 2020, the EU activated the EEAS Rapid Alert System in order to tackle disinformation campaigns related to the COVID-19 crisis. European Commission Vice-President Věra Jourová said that through this tool the member states, as well as EU partners within the G7, can share knowledge among themselves about false information “coming from external sources”.⁴

Furthermore, during a video conference of the EU foreign ministers, which took place on 3 April 2020, the High Representative for Foreign and Security Policy Josep Borrell emphasised on the importance of fighting disinformation. He stated that: “We are facing an info-demic with dangerous impact on public health. We’ll continue to tackle disinformation, and coordinate and intensify our efforts with the Member States and with social media platforms.”⁵

¹ <https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19>

² <https://www.euractiv.com/section/global-europe/news/russia-deploying-coronavirus-disinformation-to-sow-panic-in-west-eu-document-says/>

³ <https://apnews.com/02a7eb3ffeaaca022e9651ab019d738b>

⁴ <https://www.euractiv.com/section/digital/news/eu-alert-triggered-after-coronavirus-disinformation-campaign/>

⁵ <https://www.consilium.europa.eu/en/meetings/fac/2020/04/03/>

State of play

The EU's approach towards hybrid threats and disinformation

Hybrid threats posed by Russia, but also by other international actors, have been one of the EU's main security challenges in the past decade⁶ and has the potential to remain as such in the years to come. According to the Council of the European Union, these actions are conducted in a coordinated manner by hostile state or non-state actors who aim to destabilise their opponents through cyberattacks, election interference and disinformation campaigns.⁷ A briefing paper published by the European Court of Auditors includes the issue of disinformation among the cybersecurity challenges the EU is currently facing.⁸

In 2015, the EU recognised the threat posed by the disinformation campaigns, which are deployed by Russia.⁹ As a measure to counter this threat, the East Strategic Communication Task Force (East StratCom Task Force) was established within the European External Action Service (EEAS) with the purpose to address and raise awareness on the issue of disinformation.¹⁰ As a result, the EUvsDisinfo project was launched through the East StratCom Task Force in order to “better forecast, address, and respond to the Russian Federation’s ongoing disinformation campaigns affecting the European Union, its Member States, and countries in the shared neighbourhood.”¹¹

One year later, the EU adopted a joint framework on countering hybrid threats which led to the creation of the Hybrid Fusion Cell within the EEAS. The primary function of the Hybrid Fusion Cell is to provide analysis of disinformation trends to the EU institutions.¹²

In January 2018, the European Commission established a High Level Expert Group (HLEG) on fake news and online disinformation “to advise on policy initiatives to counter fake news and disinformation spread online”¹³. The HLEG was composed of representatives of civil society, social media platforms and news media organisations, as well as journalists and academia. As such, the HLEG produced a report which recommends “a multi-dimensional approach to disinformation.”¹⁴

In September 2018, the European Commission announced the release of the EU Code of Practice on Disinformation which was signed by representatives of online platforms including Facebook, Twitter,

⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018&from=EN>

⁷ <https://www.consilium.europa.eu/en/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/>

⁸ https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

⁹ <https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf>

¹⁰ https://ecas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en

¹¹ <https://euvdisinfo.eu/about/>

¹² https://ecas.europa.eu/diplomatic-network/european-neighbourhood-policy-enp/59411/countering-disinformation_en

¹³ <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>

¹⁴ Idem 13

HYBRID THREATS IN TIMES OF COVID-19: HOW IS THE EU RESPONDING TO THE RUSSIAN-DRIVEN DISINFORMATION CAMPAIGN?

Google and Mozilla. Through this code, the signatories agreed, on a voluntary basis, to ensure transparency on their platforms by increasing the visibility of reliable and trustworthy news content.¹⁵

Two months later, in December 2018, the European Commission and the High Representative for Foreign and Security Policy published an “Action Plan on disinformation” which covers four main areas: improved detection; coordinated response; online platforms and industry; and raising awareness and empowering citizens.¹⁶ This Action Plan also laid the groundwork for the creation of the EEAS Rapid Alert System as a measure “to facilitate the sharing of insights related to disinformation campaigns and coordinate responses”.¹⁷

The EU’s efforts to tackle Russian disinformation at home and abroad

The European Union Global Strategy states that the EU “will offer rapid, factual rebuttals of disinformation”¹⁸ and “will continue fostering an open and inquiring media environment within and beyond the EU, also working with local players and through social media.”¹⁹

Furthermore, the Action Plan on disinformation underlines the importance of media literacy as a method to provide citizens with the tools to distinguish real from false information and thus to build resilience against disinformation. This document also highlights the role played by civil society in raising awareness and countering disinformation.²⁰

Perhaps, one of the most visible and effective tools used by the EU to counter Russia’s disinformation operations in its neighbourhood is the EUvsDisinfo platform, the flagship project of the East StratCom Task Force. Through this platform, the East StratCom Task Force analyses and debunks false information disseminated by pro-Kremlin media outlets, while also promoting positive messages about the EU’s policies and projects in its neighbouring countries, including Russia. Initially established to cover only the EU’s Eastern neighbourhood, today EUvsDisinfo also monitors and exposes disinformation cases in the Western Balkans and the EU’s Southern neighbourhood.²¹

On 1 April 2020, the East StratCom Task Force published a special report on disinformation about the COVID-19 pandemic which provides an overview of the trending false narratives circulating in the EU member states and its neighbourhood.²² Moreover, this report contains a link to all the disinformation cases related to the crisis collected by the East StratCom Task Force since 22 January 2020.²³

¹⁵ <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>

¹⁶ https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf

¹⁷ https://eeas.europa.eu/sites/eeas/files/ras_factsheet_march_2019_0.pdf

¹⁸ http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

¹⁹ Idem 18

²⁰ Idem 14

²¹ <https://euvsdisinfo.eu/>

²² <https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic/>

²³ https://euvsdisinfo.eu/disinformation-cases/?text=coronavirus&date=&disinfo_language%25255B%25255D=ara&disinfo_language%25255B%25255D=eng

HYBRID THREATS IN TIMES OF COVID-19: HOW IS THE EU RESPONDING TO THE RUSSIAN-DRIVEN DISINFORMATION CAMPAIGN?

In parallel with the East StratCom Task Force activities, the EU has compiled a list of official information sources in all the EU member states as well as in Norway, Iceland and the UK to ensure the access to accurate and reliable news about COVID-19, in addition to the activation of the EEAS Rapid Alert System on 3 March.²⁴

The Kremlin's disinformation campaign: tactics and messages

According to the East StratCom Task Force, disinformation operations deployed by Russia during the COVID-19 outbreak are targeting both Russian and international audiences. The goal of these operation is not to only to showcase the Russian government's contribution to the fight against the virus, but also to “amplify divisions, sow distrust and chaos, and exacerbate crisis situations and issues of public concern”.²⁵

Pro-Kremlin media are playing a pivotal role in spreading disinformation and misleading information online. For instance, most of the messages promoted by these outlets focus on conspiracy theories such as “global elites” weaponizing the virus in order to take advantage of the situation.²⁶

At the same time, researchers at the Cardiff University's centre for crime and security research have noticed the fact that instead of authoring the disinformation materials about COVID-19, the pro-Kremlin media chooses to amplify theories originating from other countries such as China and Iran. Therefore, they argue that this tactic provides Russia with the opportunity to deny allegations regarding the creation of disinformation.²⁷ In that sense, the Russian president's spokesperson Dmitry Peskov stated: “We're talking again about some unfounded allegations which in the current situation are probably the result of an anti-Russian obsession.”²⁸

Conclusion

Disinformation operations deployed by Russia have proven to create significant security risks for the EU in recent years, and with the coronavirus outbreak, these risks seem to have amplified. On the one hand, by working with relevant stakeholders from the tech industry, in particular online platforms, and civil society, the EU has made meaningful progress in its efforts to tackle disinformation which includes the creation of the East StratCom Task Force, the release of the EU Code of Practice on Disinformation or the launch of the Action Plan on disinformation.

This progress has not only strengthened the EU capabilities to identify and debunk disinformation, but also to support media literacy both within its borders and beyond. On the other hand, the European Commission argues that additional steps are required, calling for “adequate human and financial

[&disinfo_language%25255B%25255D=fra&disinfo_language%25255B%25255D=ger&disinfo_language%25255B%25255D=ita&disinfo_language%25255B%25255D=spa](#)

²⁴ <https://www.ecdc.europa.eu/en/novel-coronavirus-china/sources-updated>

²⁵ Idem 22

²⁶ Ibid

²⁷ <https://www.theguardian.com/world/2020/mar/18/russian-media-spreading-covid-19-disinformation>

²⁸ <https://www.dw.com/en/russia-denies-eu-allegations-over-coronavirus-disinformation-campaign/a-52825640>

HYBRID THREATS IN TIMES OF COVID-19: HOW IS THE EU RESPONDING TO THE RUSSIAN-DRIVEN DISINFORMATION CAMPAIGN?

resources to better detect, analyse and expose disinformation campaigns and raising preparedness to address disinformation campaigns at EU and national level”.²⁹

The final report of the HLEG on fake news and online disinformation defines disinformation as “a multifaceted and evolving problem that does not have one single root cause. It does not have, therefore, one single solution.”³⁰

The unprecedented challenges posed by the pandemic coupled with the rapid technological developments makes it difficult to determine the impact it will have on the EU’s approach towards disinformation and hybrid threats in general, but to some extent, it can shape the ability of the Union and its member states to better counter disinformation while also protecting freedom of expression and increasing transparency.

The Action Plan on disinformation and the final report of the HLEG seemingly establishes the promotion of media literacy as a long-term priority for the EU in order to increase resilience to fake news and misleading information. Taking into account that building resilience is a key priority in the European Union Global Strategy, focusing on fostering media literacy might be an appropriate course of action for the EU to pursue in the future as it has the potential to allow the Union to make important strides in tackling disinformation while also being able to protect its core values.

²⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52019JC0012&from=EN>

³⁰ <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>

HYBRID THREATS IN TIMES OF COVID-19: HOW IS THE EU RESPONDING TO THE RUSSIAN-DRIVEN DISINFORMATION CAMPAIGN?

VOCAL EUROPE

RUE DE LA SCIENCE 14B, 1040 BRUSSELS

TEL: +32 02 588 00 14

VOCALEUROPE.EU



[TWITTER.COM/THEVOCAL EUROPE](https://twitter.com/thevocaleurope)



[FACEBOOK.COM/VOCAL EUROPE](https://facebook.com/vocaleurope)



[YOUTUBE.COM/VOCAL EUROPE](https://youtube.com/vocaleurope)



[INSTAGRAM.COM/VOCAL EUROPE](https://instagram.com/vocaleurope)

Disclaimer and Copyright

This document is prepared for, and addressed to Vocal Europe and its audience. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of Vocal Europe. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged.