PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 104 (1800), 26 MAY 2021 © PISM

BULLETIN

EU Sanctions for Disinformation Campaigns: Prospects and Limits

Elżbieta Kaca

The EU has faced a growing number of foreign disinformation operations, mainly instigated by Russia and China. The European Commission (EC) is considering a sanctions system in response to such attacks. Its would, however, be limited by technical difficulties in detecting the sources of such operations and Member States' divergent views as to the scale of retaliation. From Poland's perspective as a country supportive of using sanctions in EU external relations, such a solution would strengthen the EU's response to Russian and Chinese hostile actions.

In December 2020, in an EC communication on the European democracy action plan, the Commission proposed exploring the option of using EU sanctions in response to foreign operations in the information space that are detrimental to the Union. They would apply to covert campaigns undertaken by states and their representatives that use disinformation, meaning the deliberate dissemination of false or misleading content, and other manipulation techniques.

The reason behind the EC's proposal is the growing wave of disinformation visible in the EU during the COVID-19 pandemic, and mainly instigated by Russia and China. The campaigns aim to undermine confidence in Western vaccines (mainly the newer mRNA type), EU institutions and vaccination strategies, and fuel the anti-vaccine movement. Russia has carried out many operations during election periods, for example, in 2016 amid the referendum on the UK's exit from the EU, and in 2017 during the presidential elections in France and parliamentary elections in Germany.

The Specificity of the Threats and Their Detection. The purpose of disinformation operations is to achieve political or economic benefits by undermining public confidence in democratic institutions in this case and increasing socio-political divisions. When it comes to the narratives, foreign entities most often seek to demean European democratic values, politicians and institutions, propagate conspiracy theories, or promote the view of the EU's supposed disintegration. The main tool of such disinformation is use of social media via fake accounts, trolls, and bots, most often on multiple platforms at the same time. Since the beginning of the COVID-19 pandemic, at least 740 examples of Russian disinformation have been identified in the EU, such as articles successfully popularised on social media (East StratCom Task Force data). In Germany, nearly 3,000 Russian-sponsored accounts engaging in election-related discussions were identified in 2017, and 7.4% of Twitter feeds on this topic were generated by bots.

The entities conducting these disinformation operations constantly improve their methods to gain popularity among the target recipients and make detection difficult. Fake accounts, websites or groups are profiled in a such a way as to reach their targets. They might give the impression that they are independent institutions, think tanks or research initiatives, or build up an image as a trusted public figure. They also operate on encrypted platforms like WhatsApp, closed Facebook groups, and websites like Reddit, and they use AI-generated profile pictures that make it difficult to identify the operations. States that engage in disinformation have increasingly outsourced these campaigns to private companies, particularly marketing firms. During the 2020 U.S. elections, the Russian operation

used newly established companies in Ghana, Mexico, and Nigeria.

The largest social media platforms, mainly Facebook and Twitter, have been detecting an increase in disinformation campaigns and remove some of the content. However, they are quite selective. As these platforms derive most of their income from advertising, they only reveal a bit about operations carried out by economically important countries, such as China. According to the Global Disinformation Index, the advertising revenues just from websites promoting disinformation targeting EU countries amounted to $76 million in 2020. At the EU level, East StratCom monitors mainly Russian disinformation. The Member States, particularly Czechia, Estonia, Finland, France, Lithuania, Germany, and Sweden, are increasingly developing their own investigative capacities in this field. Numerous non-governmental organisations and scientific institutions in the EU work to detect disinformation using open source methods. The EC supports financially the European Digital Media Observatory, which operates in this area. However, such analyses are hampered by the lack of regular access to the data of social media platforms.

Possible Scope of Sanctions and Challenges. A sanctions model to follow would be the EU restrictions system introduced in 2019 to respond to cyberattacks. It could include an EU entry ban and assets freezes on natural or legal persons directly responsible for, providing support to, or otherwise involved in the implementation of a disinformation campaign. The sanctions could be applied to operations based outside the EU and its Member States that pose serious repercussions within the Union. Examples of this include campaigns carried out during election periods and/or against socio-political institutions. The regulation should allow the use of restrictions in cases of other violations connected to the disinformation, without specifying them, as campaigns can be implemented during unforeseen crises. Moreover, the EU should be able to apply sanctions in response to major operations against third countries or international organisations. The regulation may also specify factors to measure the impact of a campaign. Although this is difficult due to the inability to directly examine the views of disinformation recipients, there are many methods for assessing an operation's effects, such as the popularity ("likes") of accounts and entries, or the scale of their duplication by various media and social circles among, for example, traditional media and decision-makers.

It will be problematic to attribute an operation to a specific entity and provide sufficient evidence by the legal services of the Council of the EU in this respect. In order to confirm the source of a campaign, access will be needed to classified information from Member States' intelligence services on suspicious entities, as well as to technical data of social media platforms, including accounts, administrators, or the software or infrastructure used. Platforms may share such information at the request of the law enforcement authorities of a given country. Member States' intelligence services, however, are reluctant to cooperate at the EU level in countering disinformation. Although there are channels for the exchange of classified information, such as the Hybrid Fusion Cell at the EU Intelligence and Situation Centre or the Rapid Alert System, which provides early warning of disinformation campaigns, only some countries actively engage in this kind of cooperation. Even if sufficient evidence is collected to attribute an operation, it may be difficult to gain the unanimity necessary to adopt sanctions by Member States due to their divergent attitudes towards certain countries, such as Russia and China. Some countries, for example Hungary or Cyprus, are reluctant to apply such restrictions due to their own interests, and may officially block the instrument. Other states, including Poland, the Baltic states, Czechia, and Slovakia, which emphasise the security threats posed by Russia and/or China, are more likely to support the launch of such restrictions.

Conclusions. The Member States' support for the introduction of the sanctions system will depend on the effects of disinformation regarding the COVID-19 pandemic and the scale of future operations during election periods in the largest EU countries. As the restrictions would officially assign the source of the attacks, they would be advantageous in terms of reaffirming the EU's unity in the face of new threats and increasing public awareness of foreign interference in the information space.

On a technical level, it will be important to increase the detection of disinformation campaigns. In the negotiated act on digital services, Member States should agree to introduce an obligation for online platforms to provide data on illegal content and deliberate manipulation to the EC and verified researchers. They can also extend East StratCom's mandate to monitor disinformation from China and other third countries, which requires an increase in the Task Force's modest budget. It will be important to exchange information between the Member States and also with the U.S., given its experience in detecting the sources of operations, as evidenced by the sanctions against Russia in April 2021.

From the perspective of Poland, a target of Russian and Chinese disinformation campaigns, EU restrictions would be a useful instrument to pressure the authorities of these countries. Poland can promote the mechanism in cooperation with the Special Committee on Foreign Interference in all Democratic Processes in the EU, including Disinformation (INGE) in the European Parliament, which is the body that recommends the introduction of sanctions.