Council of the European Union
General Secretariat

Brussels, 20 April 2021

Interinstitutional files:
2020/0361 (COD)

WK 5285/2021 INIT

LIMITE

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC 20/01/2022

COMPET
MI
JAI
TELECOM

CT
PI
AUDIO
CONSOM
CODEC

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	LV Delegation
To:	Working Party on Competitiveness and Growth (Internal Market - Attachés) Working Party on Competitiveness and Growth (Internal Market)
Subject:	NATO Strategic Communications Centre of Excellence - On Article 31 of the Digital Services Act

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

Street Kalnciema 11B, Riga, LV-1048, Latvia
Ph. +371 67335467; e-mail: info@stratcomcoe.org

Riga, 7 April 2021

No. SCCOE-R-21/2-19/12

Ministry of Economics
Republic of Latvia

Subject: On Article 31 of the Digital Services Act.

First of all, let me express my gratitude for having an opportunity to express our view on the Article 31 of the Digital Services Act.

Article 31 stipulates that, in order to assess and monitor compliance with the regulation, large platforms should upon request provide data to vetted researchers, who would conduct research contributing to the identification and understanding of systemic risks. Amongst the identified systemic risks are the 'intentional manipulation of their service, including by means of inauthentic use or automated exploitation' with a 'negative effect on the protection of public health, minors, civic discourse, or foreseeable effects related to electoral processes and public security'.

These are very much an area in which the NATO Strategic Communications Centre of Excellence has expertise in. See, for instance, our ongoing *Robotrolling* reports, or the 2019 *"Falling behind: how social media companies are failing to combat inauthentic behaviour online"*. However, Article 31 proceeds to specify that the researchers working with these data should be affiliated with academic institutions.

Our report *"Falling behind"* takes the Code of Practice on Disinformation as the starting point to assess how effectively social media companies combat fake activity on their platforms. It used an experimental methods whereby we commissioned activity by fake commercial social media accounts. After identifying fake accounts, we tracked whether the companies' algorithms were able to detect and remove them. We also assessed responsiveness when we reported the accounts as fake. The results, unfortunately, revealed eye-opening failures in both cases.

Having done these experiments, we see that self-regulation is not solving the problem. In the report we call for better auditing of social media companies' responses to such activity. The incentives for removing fake activity from social media platforms are not strong enough - fake accounts also generate ad-revenue.

Therefore, our work is greatly enhanced by the data access outlined in the DSA. Examples include but are not limited to:

1. Ad data: What ads had these accounts been shown? Which companies had lost the most in ad spend as a result?
2. User activity: What pages, political candidates, influencers, etc. had these accounts promoted? How many citizens interacted with the activity?
3. Log data: to determine whether these were coordinated, automated, worked as a cluster, were operated out of a single location, etc.
4. Deleted accounts: understand the behaviour of accounts that were identified and removed by the platform.
5. View / interaction data: whether the activity by fake commercial accounts successfully caused posts to trend / go viral.

Unfortunately, we see that the current wording of Article 31 would appear to prevent such work. Therefore, we would be grateful if the Article 31 could be amended the way it does not exclude organisations as ours, from accessing data for research.