European
Commission

Julian KING
Member of the European Commission

Rue de la Loi, 200
B-1049 Brussels
Tel. +32 2 295 74 20
julian.king@ec.europa.eu

Brussels, 19 March 2018

Ms Mariya Gabriel
Commissioner for Digital Economy and Society

Dear Commissioner Gabriel,

I was sorry to have missed your working breakfast and the last Project Team discussion on the Communication on fake news you are currently preparing, so I wanted to briefly set out some of my thinking from a security perspective.

It is clear that the cybersecurity threat we are facing is changing from one primarily targeting systems to one that is also increasingly about deploying cyber means to manipulate behaviour, deepen societal divides, subvert our democratic systems and raise questions about our democratic institutions. The seriousness of this threat and the security risks that come with it are also clearer than ever before. This weekend's revelations about the psychometric targeting activities of Cambridge Analytica using mined Facebook user data are a further example of exactly what we are up against.

Unfortunately, it is likely that such activities are only a preview of the profoundly disturbing effects such disinformation could have on the functioning of liberal democracies, which are built and rely on the possibility to exchange and receive reliable information in an open and shared public sphere.

As you know, Member States are also growing increasingly concerned about this phenomenon, prompting France to prepare a legislative proposal on this issue. In light of this as well as the strategic nature of this threat and the upcoming EU elections, your work on the Communication is both timely and essential in terms of providing a clear and firm answer, based on a careful and solid definition of the problem, and I would like to reiterate my full support in this process.

I read with great interest the recently published report of the independent High-Level Expert Group and I would like to commend your effort to set up an inclusive process, in which all relevant actors are involved, ensuring that all dimensions of this complex issue are well understood and addressed.

In terms of problem definition, a consensus appears to have emerged: disinformation is nothing new but in today's cyber connected world it has become far easier, quicker and more effective both in terms of scale and impact. We are faced with a diverse range of malicious actors seeking to harm us – private citizens, companies, state actors, non-state actors — who are successfully harnessing new techniques that allow the reach of a message to be dramatically increased and its impact similarly amplified, by targeting it at specific audiences and continuously exposing the same people to the same type of messages. In short: it is the results of powerful social media tools put in the wrong hands, notably those of algorithms, 'trolls' and 'bots'.

It is clear that we need to become collectively more resilient to this phenomenon by strengthening all sources of independent and verified information, by raising awareness and by teaching critical thinking on a much wider scale, so that these surreptitious campaigns meet less fertile ground.

But to achieve real and rapid results, it is crucial that we urgently address two main structural aspects: influencing the behaviour of those who are behind such campaigns and looking into the use and functioning of infrastructures conveying and amplifying such content. In this context I believe a key element of our response against disinformation should be reinforcing online accountability. In the offline world, freedom of speech and the freedom to conduct business both come with accountability. This should also be the case online.

For Internet platforms and the advertising industry, this means taking appropriate measures to prevent disinformation from being widely spread – while fully respecting freedom of speech – and from being a source of revenue. In particular, this requires greater transparency about the role and impact of algorithms – to help avoid the phenomenon of "algorithmic confinement" and as well as abiding by strict rules in terms of whom data can be sold to – to avoid the Cambridge Analytica effect.

On this issue, experience suggests that a self-regulatory approach is likely to prove insufficient. A more binding approach – with at least some clearly and carefully defined performance indicators – should be considered, especially in order to:

- Compel platforms to provide real transparency on sponsored content (identity of the sponsor, amounts spent to promote the content), in particular during electoral campaigns ;
- Distinguish sponsored content (which should always appear as such) from other content ;
- Enforce the "follow-the-money" principle, to prevent incentives that lead to disinformation; and
- Further limit the possibilities for using mined personal information for certain specific purposes, in particular political ones.

For individuals, this means putting in place mechanisms to ensure more accountability for content posted or disseminated online. Indeed, disinformation campaigns as well as cyberattacks are largely enabled and encouraged by the lack of traceability and accountability currently enjoyed by perpetrators.

In this regard, voluntary systems to allow for verified identification and authentication should be part of the debate around disinformation. Identification solutions could be a powerful tool to change the atmosphere of cyberspace and increase trust between users. The work we are doing jointly in this area (to preserve the WHOIS database of domain name owners and develop IPv6, which allows the attribution of one IP address per user) could be complemented by other innovative approaches, such as projects to enable privacy-preserving Internet real-name registration, thus reconciling anonymity with responsibility on the Internet through "verified pseudonymity" or other identification mechanisms compliant with data protection regimes.

In parallel, we need to set up a comprehensive cybersecurity strategy to prepare for the upcoming European elections. Disinformation now forms part of a wider array of cyber-manipulation tools that can affect electoral processes, such as hacking or defacing websites or gaining access to and leaking personal information about politicians. As ever in the field of security, the primary responsibility lies with Member States, but I believe we should support their work at EU level with for instance the definition of concrete guidelines for authorities, the media and online platforms so that, come May 2019, we all have clear roles and a clear game plan.

In the mid-term, I also think there is a strong case for our electoral rules to be reviewed and looked at through this new cyber lens.

The possible consequences of disinformation – the undermining or delegitimising of democratic institutions, for example – are a serious, strategic and growing threat; a key part of the security challenge we face today. I am confident that your proposals will frame this debate in a comprehensive way and will put forward concrete and convincing answers, in line with the extremely important stakes.

Yours sincerely,

[redacted]

Julian KING

CC:
First Vice-President Frans Timmermans
Vice-President/High Representative Federica Mogherini
Vice-President Andrus Ansip
Vice-President Jyrki Katainen
Commissioner Günther Oettinger
Commissioner Cecilia Malmström
Commissioner Vytenis Andriukaitis
Commissioner Dimitris Avramopoulos
Commissioner Marianne Thyssen
Commissioner Pierre Moscovici
Commissioner Violeta Bulc
Commissioner Elżbieta Bieńkowska
Commissioner Věra Jourová
Commissioner Tibor Navracsics
Commissioner Corina Crețu
Commissioner Margrethe Vestager
Commissioner Carlos Moedas
Secretary General Martin Selmayr
Director General Paraskevi Michou
Director General Roberto Viola
Director William Sleath
Member of President Juncker's Cabinet Michael Shotter