ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

COMMENTARY
23.05.2019

THE EU AND DISINFORMATION: A BATTLE TO BE WON TOGETHER

Fabio Rugge
ISPI

During the March meeting of the European Council there was talk once again of disinformation, the threat it poses (especially when conveyed through social media) and the risk that it could be used to influence the democratic process, both nationally and in the imminent elections for the European Parliament. In other words, just a few weeks after the European Parliament had passed the Cybersecurity Act[1] (a significant step towards greater cybernetic security for Europe's citizens and businesses), threats from the cybersphere returned to the European institutional agenda, telling of a need – unmet, in this case, by any significant decisions – to stay highly alert to what is evidently perceived as a real and present danger. And no wonder: for constant vigilance is, we know, the primary duty of any open democracy.

How serious, then, are these risks? The cybersphere has taken a traditional danger – psychological warfare – and raised it to a new level by making it far more pervasive, firstly because – as anyone who has ever visited a chat room can testify – online behaviour can so easily be anonymous, unfiltered, and unhampered by social conventions in a way which would be unthinkable "in real life". Secondly, the Internet's impact is non-linear: by its nature ("the medium is the message") it fosters distorted news and information; its tendency is to serve up whatever suits and accordingly strengthens pre-existing views of the world (and strengthens preconceptions even more).

This polarizes public opinion and feeds divergent "truths" in public debate, undermining the basis of any opportunity for genuine, informed discussion. For democracy, whose life-blood is the public expression of opinion by citizens who want to participate in political life in a spirit of honest argument, this is a threat to its very existence. Forces outside the Union can exploit these intrinsic vulnerabilities for hostile purposes: to influence public opinion on a particular matter of national interest, for instance, or to delegitimize unfavoured candidates for office, or to stir up popular revolt by orchestrating messages which push people's most sensitive emotional buttons at the moment. This can all be done using totally bogus "news": the technology already exists, for instance, for the near-perfect digital re-shaping of a public person to make it spout whatever messages go down best.

This article was originally published in the ISPI-IAI Observatory on Italian Foreign Policy

The expressed opinions reflect only the author's views.

Thirdly, the cybersphere adds another degree of risk by making it possible to profile users according to their opinions (harvested and checked, and/or presumable), so as to maximize the effectiveness of disinformation campaigns. Online propaganda can moreover be automated by using "bots" (special algorithms which get "smarter" and more autonomous every day), or by tweaking or stealing sensitive data from computers compromised by the latest cyberweapons (which may have been bought anonymously on the *Dark Web*), with the aim of subsequently exposing such sensitive data online, more or less selected and/or toned down, at the strategic moment.

In last December's Joint Communication to the Parliament, the Commission and Council of the European Union adopted a "Plan of Action against Disinformation". The Plan identified four main lines of action: improving the capabilities of EU institutions and member states to detect, analyse and expose disinformation; strengthening their coordinated responses to disinformation; putting responsibilities on the operators of digital platforms; and involving individuals, think tanks and universities in the work of preparing a "*common picture*" of any co-ordinated disinformation activities detected on the digital services used by European citizens.

The Plan has already been put into practice: a Rapid Alert System went live on 18 March. In brief, this is a digital platform that will facilitate interaction among all the main stakeholders, both European and national, to exchange information in real time about current disinformation campaigns and coordinate the response to them. In the face of an asymmetric threat like *cyber-enabled information warfare*, teamwork is the most important advantage available to the defence: so the measures taken by the EU are valuable and all the more urgent because the various member states still have no clear strategy or national code of operating procedures to tackle this threat.

Because of these and other strategic considerations, Italy, for its part, has not been slow to actively support these developments and to reiterate whenever possible the need for complementarity between what the European Union is doing and what is being done in NATO. The latter has in fact for some while been paying special attention to hostile disinformation campaigns precisely because they can severely affect decision-making processes and allied solidarity, not least as one definitional component of what is known as "*hybrid warfare*". This has led to a demand for the two organizations to work productively together across the entire range of the potential threat, avoiding harmful duplications and also ensuring consistency in all those areas which may not directly concern disinformation, but which certainly can aggravate it: one thinks of the EU's adoption of the NIS Directive and the GDPR, or the strengthening of intelligence-sharing and the activation of specific military *indicators & warnings*.

Lastly, in the months leading up to the European elections, the Plan of Action requires operators of online platforms to report on what they are doing to stop disinformation campaigns using their systems. Those operators' involvement and their proper discharge of all their responsibilities are essential for practical results, and clearly the EU is in a better position than individual member states to talk to *over the top* operators. In this sense, the prevention of disinformation campaigns is yet another illustration of how the international security situation requires strong actors capable of speaking with a united voice. "Everyone for himself" is in fact an impossible defence when the threat comes over networks which are interlinked by their very nature.

As always, our effective membership of the EU does not replace the "homework" we need to do ourselves; a national effort is needed, especially in terms of education and the raising of awareness,[2] starting with our schools but extending to all occupations and to civil society in general. With correct information and its characteristic critical spirit, Italian public opinion will certainly be capable of responding to needs articulated in Brussels, but it will be our hard put-upon democracies that feel the benefit of the exercise.

[1] S. Dominioni, "The EU Cybersecurity Act: When the Going Gets Tough, the Tough Get Going", ISPI Commentary, 18 April 2018.

[2] F. Rugge and S. Dominioni, "Cybersecurity in Italia: il nodo della formazione", ISPI Commentary, 7 February 2019.