Journalism's key role in history – Information in the digital era – The manipulation of information – Fake news – Disinformation campaigns – How to combat manipulation – Responsibility of digital platforms – EU action – Combating interference in the democratic process

Digital sector – International conference, "Civil societies, media and public authorities: democracies facing the manipulation of information" – Closing speech by M. Jean-Yves Le Drian, Minister for Europe and Foreign Affairs

Paris, 4 April 2018

I'm happy to be concluding this afternoon of discussions and dialogue on an issue which, in the space of a few years, has become one of the most important and also urgent ones we're being called on to address. I'm going to conclude – I'm sorry about this – at some length, but the issue does deserve a minimum amount of consideration. I especially thank the CAPS [Centre for Analysis, Planning and Strategy], several members of which, I know, played an active role in the preparations for and the success of this day.

JOURNALISM'S KEY ROLE IN HISTORY

The issue concerns us all – and by "us" I mean the public authorities, political leaders, the leaders of voluntary organizations, media professionals, players in the digital world, researchers, teachers and citizens themselves. In short, everyone who knows that there are such close ties between information and democracy that neither can exist without the other, and that there can be no democratic life without a public space fuelled by the work of journalists, any more than there can be information without institutions and rules which guarantee its freedom, independence and legitimacy in the eyes of our fellow citizens.

To mention only the case of France, in each of the founding moments of our Republic – and very often they were also moments of crisis, of intense questioning of our democracy's very meaning –, journalists played a leading role. It was about clarifying the public debate, always with the same demand for reason, indissociable from the search for autonomy that characterizes modern citizenship. For one major reason: the precondition of autonomy is access to information, so that citizens can freely exercise their judgment.

In these critical times, journalists and press outlets have responded to this need to know and understand. There would have been no Dreyfus Affair, just an innocent man condemned and forgotten by everyone, if Bernard Lazare, true to his idea of journalism, hadn't been among the first to try to restore the truth by dismantling, point by point, the treason accusation levelled against Captain Dreyfus by the military court.

During the Second World War, the Occupation would have been complete darkness without the voice of Radio London and those of Maurice Schumann, René Cassin and Pierre Brossolette, who gave shape to the political project of Free France. The French wouldn't have had the same perception of the Algerian War without the work of Françoise Giroud and Jean-Jacques Servan-Schreiber denouncing torture. These examples – and there are many more – show the extent to which journalism is an instrument of freedom without which citizenship cannot be exercised in an enlightened way.

At a time when major upheavals are transforming the information sphere, we're entering this new world, aware of how far previous technical revolutions – mass press distribution and the invention of radio and then television – were instruments of progress and democratization in our societies. "Reading the newspaper is the modern man's morning prayer," said Hegel.

Last century's battles for emancipation and today's battles to increase human autonomy all echo, in their way, the truth of this phrase, written at the dawn of our modern political era. Media revolutions have massively heightened their impact, by providing access for an ever-broader public to an increasingly vast world of information and knowledge.

INFORMATION IN THE DIGITAL ERA

The emergence of a global digital space is once again shaking up every sector of human activity. It's become a fully-fledged area for conducting international relations in every field, particularly that of soft power and public diplomacy. The Quai d'Orsay has resolutely embraced this digital turning point. With more than a million followers, the Foreign Ministry's Twitter account is the second most followed institutional account in France; it now appears in five foreign languages, with the advent of Russian a few months ago. I also want to mention France Médias Monde, which disseminates the basics of our culture worldwide. Today the Internet and social media have created a new way of organizing information and its circulation, whereby a player's clout is determined by their audiences and impact.

In the last decade, new actors have emerged in the information sector, conquered the market and divided it into cartels. Today we're facing a situation of duopoly, because access to the press and information is mostly provided via Google and Facebook. These two platforms have a market power unlike anything that any press outlet has had in past decades. The public space is being transformed by them, as are shifts in opinion and the way opinion is formed. So they're becoming central to democratic life and the organization of life in society itself.

The revolutions of the Arab Spring showed how far social media could act as a galvanizing force. Today we're seeing the extent to which the free Internet access, freedom of expression and freedom of information that digital tools provide over a far greater spectrum of time and space are also being targeted by political authoritarianism.

In the information field, I believe the digital space has developed along three lines of tension which are now reaching their peak: firstly, tension between the promise of openness and the new manipulations this openness enables; secondly, tension between free access to an infinite volume of information and the reality of a fragmented digital world divided into information silos, where contradictory discussion is weakened; and finally, tension between a decline in production and distribution costs which theoretically facilitates the emergence of new information players and the fragmentation of sources themselves, with widespread doubt about the reliability of the information distributed.

MANIPULATION OF INFORMATION

In this new information age, democracy must answer the question it has faced since its origins, the question Socrates was already asking the Sophists: how can we safeguard opinion against the power of fakery and those who trade in it?

In setting out France's international digital strategy last December, I said the digital space bears the promise of progress; and I strongly believe this: it can breathe new life into our democratic values. But it's also a source of new risks, particularly that of digital information that is manipulated to contradict the virtues of openness and progress that we recognize in it.

The unprecedented nature of the situation we're facing results from a combination of three factors: firstly, the crises and doubts that have been gripping our democracies for a decade; secondly, the revolution represented by the digitization of the public space, a shift which further amplifies the questions and tensions gripping our societies; and finally, the ever-clearer assertion of power strategies ruthlessly using digital destabilization strategies exercised in the information sphere. I also note that some statements, such as that written by Russia's chief of defence staff in February 2013, describe "informational actions" as a possible instrument in the external intervention toolbox.

Our democracies have been slow to realize the gravity of this phenomenon. And yet we've noticed how, in open conflicts including on the European continent, digital tools are being used to bring confrontation all the way into the information sphere. This reality has taken on a new aspect in the digital era: we've entered a new propaganda age. The management of news about the crisis in Ukraine and the operation to annex Crimea was a major alarm call. Awareness increased with a string of misfortunes in recent elections, including in France. In the United Kingdom, the United States, France and Spain, the ballots were all characterized by the spread of fake news and computer attacks aimed at disturbing public order, compromising the integrity of the vote and thus sowing doubt and discord within the Western democratic system.

Driven by a cynical vision of the digital space, those who engage in these manoeuvres are trying to turn against our democracies their very founding principles – openness, freedom of expression and information – with a view to interference and destabilization. Disinformation and the existence of propaganda media outlets are not a new phenomenon, of course, but they've acquired unprecedented significance thanks to the digital revolution and its impact on the way the public – especially our young people – are informed.

FAKE NEWS

The public debate has crystallized around the notion of fake news. This issue worries me and concerns the orchestration of digital strategies of interference and informational destabilization, and I think this new category adds to the current confusion rather than allowing us to identify precisely the threat our democracies are facing. The shortcoming of the notion is that it tends to encompass phenomena of a different nature, and motivations and consequences that bear no relation to one another.

Fake news may be fake for various reasons: by accident, through carelessless, or through its gradual distortion as it spreads and is repeatedly relayed to the point of becoming online rumour. It can also be intentional without being politically motivated, either because it's a hoax or because it's a source of income. There's a risk of information in the digital space giving a comparative advantage to the most sensational content, which is consequently liable to be picked up and widely shared, with the advantage this represents for advertisers. Likes, retweets and shares pay. And they generally pay well.

Fake news can also be issued for malicious purposes – this was mentioned earlier at a round table I attended – to compromise the online reputation of a person, group or business. The rise of conspiracy theories is one of its most worrying manifestations.

But the most serious case is when fake news is part of a comprehensive strategy, an action with strategic significance aimed at destabilizing institutions themselves by targeting a

population. Here the term "fake news" is inappropriate and insufficient; it must be replaced by the term "manipulation of information", which I propose to define on the basis of three criteria. Firstly, it's an orchestrated campaign involving both state and non-state actors. Secondly, it involves the widespread dissemination of deliberately-fabricated fake or biased news, which spreads virally because it's automated and coordinated. Thirdly, this strategic action has a hostile political objective: to dominate, interfere with and destabilize the populations, institutions and states targeted, in order to influence their choices and undermine the autonomy of their decisions and the sovereignty of their institutions.

The complexity of these tactics has to be clearly grasped. Campaigns of this kind combine both real and distorted information, as well as exaggerated facts and entirely made-up news stories. They're sometimes based on information obtained fraudulently, as was the case with the hacking of Emmanuel Macron's campaign messages or, before that, of the Democratic Party's servers in the United States.

These campaigns begin on social media with an increasingly sophisticated system of automated amplification enabling the information to spread virally. Very often, the speed at which it spreads is also an interesting indication of the phenomenon's orchestrated and automated nature.

But the most sophisticated strategies consist in creating a source of information which is reliable in nearly all cases, through the methods I highlighted, in order to render fake news credible when the time comes. The "laundering" of this counterfeit online currency of invented news, disseminated and then relayed by authorities, legitimizes them in the public's eyes.

As Defence Minister I had to handle these types of attacks – because they are attacks – when false accusations of harm to civilians were issued by Daesh [so-called ISIL], then relayed by the Syrian regime and finally reported in the press on an equal footing with the coalition's denials. I knew this was fake, because no French planes were flying to the place concerned and the photos used were of a Syrian air force bombardment. But the principle of solidarity inherent in any military coalition prohibited me from issuing denials separately from my allies. And that very solidarity was tested by this manipulation.

DISINFORMATION CAMPAIGNS

For several years, a veritable disinformation industry – and a low-cost one, incidentally – has been organized and financed, with its troll farms and systems of bots. There's nothing accidental about the targeting of democratic societies during election processes. It's a time when the public arena is under the highest tension, political passions are being fully played out and the polarization of public opinion consequently provides the greatest room for exploitation. This same objective leads the people organizing those campaigns to choose certain especially sensitive issues in order to increase divisions within the social fabric.

In recent years we've experienced the first wave of a new form of this manipulation of information. The rapid progress of artificial intelligence, the sale for modest sums of increasingly high-performance software enabling people to counterfeit videos – all these and future technological innovations will give those seeking to destabilize our democratic life new ways of interfering. They could lead disinformation across a new threshold by seeking to

manipulate the perception of reality itself, still with the same objective: to create a climate of mistrust, erode the very idea of truth and encourage the emergence of mass scepticism.

I know you've mentioned possible new methods of attack during your conference.

HOW TO COMBAT MANIPULATION

So we must find ways of addressing this challenge. It's not about letting ourselves be dragged into an information war process. But in the face of these risks and attacks, our goal should be to guarantee the resilience of the public arena by inventing a new, partnership-based, liberal model.

The starting-point for our reasoning must be the fact that democratic, liberal systems are ultimately more effective. They facilitate innovation, allow consensus, and reduce the risk of authoritarian excesses with all the corruption and therefore social ineffectiveness they create; they value merit. When all is said and done, the instruments used by authoritarian regimes to destabilize us can only have been developed in open societies. So we must remain confident in our strength, and particularly in our resilience, but at the same time adapt to confront those who wish to undermine the freedom of our democracies.

This defensive democratic model requires not only action by the public authorities but also responsibility from businesses and vigilance from civil society and the media.

Recent attempts to intefere in our presidential election and partner countries' democratic procedures are a serious violation of both the people's will and national sovereignty. The gravity of this interference cannot be underestimated. It requires measures by the public authorities to defend the integrity of the vote, so that it faithfully reflects the will of the majority of citizens.

The Culture Minister recalled this on opening this conference. It's the goal of the initiative taken by La République en Marche's parliamentary group, which has presented two bills to the National Assembly, one institutional, the other ordinary, relating to the spread of false information, especially concerning election campaign periods.

These bills will be examined over the coming weeks, and I want to commend the work done by the Cultural Affairs Committee and the committee responsible for reviewing legislation, which have taken on these issues and are going to begin their work in the next few days.

The goal of this plan is to strengthen the powers of the authorities providing all the guarantees of independence of a law-based state – judges and the Higher Council for the Audiovisual Sector – as guardians of the integrity of the vote, and to increase the cost of disinformation campaigns to their initiators. As a last resort, it will enable the regulator to suspend or definitively end, within a very short time, the spread of malicious content controlled or confirmed as being influenced by a foreign state.

Discussions of the same kind are under way among several of our close partners.

These destabilization campaigns use all the new instruments offered by the digital revolution. So the public authorities must also take action in the technological sphere.

In the short term, technology offers promising solutions for preventing, detecting and dismantling information manipulation. Thanks to the progress made on artificial intelligence, today we have increasingly high-performance tools for identifying coordinated campaigns of false information, opposing the viral spread of sensational news, combating fake accounts and securing our digital infrastructure. We're now capable of detecting disinformation campaigns upstream, tracing them back very quickly to the original source that launched the operation, viewing the network of distribution points or originators that have helped spread those hostile messages, and deactivating the false accounts that support this viral spread.

Armed with these tools, tomorrow we'll have to pursue and denounce the authors of campaigns aimed at destabilizing our country. Tomorrow we'll have to be in a position to say who runs these thousands of fake accounts, who guides the positions they take, and – when it's states, as can happen – to denounce their actions for what they are: hostile actions aimed at undermining our way of life and our institutions. Because they're generally countries which have made "non-interference" and "respect for sovereignty" the cornerstones of their international discourse, this prospect is bound to pave the way for interesting public explanations.

Without waiting for this, however, we must bear in mind that our first defence is resilience. Our behaviour must also change. In January 2017 I argued that on a daily basis everyone, particularly civil servants privy to sensitive cases, should show a kind of "computer hygiene" – i.e. adapt their behaviour to the risk of leaks that exists, whatever defences we put in place. Any computer message can be intercepted. Those who write them must constantly bear this fact in mind, even when it comes to trivial conversations.

Alongside this technological toolbox, there must be an effort to train public employees. Our institutions must equip themselves with internal expertise so as to be capable of autonomously thinking up strategies that fully integrate these dimensions. That's not yet the case today: there's a worrying asymmetry of power, resources and information between digital businesses and public institutions. This impression of a loss of control helps fuel our fellow citizens' anxieties about globalization and technological progress.

So it's urgent to think of new models of recruitment, training, public-private partnerships and our employees' mobility to innovative businesses, enabling this new knowledge to be acquired and circulate. The universities and institutions that educate senior officials in our government departments also have an essential role to play in suggesting tailored programmes.

In my ministry, the Communication and Information Directorate will be responsible for implementing a monitoring and early-warning system, so that we can react swiftly to an information-manipulation campaign targeting our interests abroad. Our reputation and the confidence we can inspire are essential assets for our diplomacy. So they're probably capable of being attacked, and it's our duty to be in a position to react very swiftly.

Within our diplomatic network, press departments especially will be called on to observe, analyse and learn lessons from any attacks our partners might undergo. At the next ambassadors' conference, I'd like us to learn lessons from this feedback and from the discussions we'll have had with all those who track manipulation on a daily basis, sometimes voluntarily. Some of them are with us, like M. Alaphilippe, who, together with his associate, Nicolas Vanderbiest, very quickly documented in the spring of 2017 the campaigns

orchestrated from Russia against the candidate Emmanuel Macron. This challenge will also be integrated into our next planning and forward-planning exercises.

Finally, my ministry's Centre for Analysis, Planning and Strategy, along with the Military Academy's Institute for Strategic Research, is currently finalizing a report bringing together the analyses and best practice of our partners, researchers, media and civil society organizations worldwide. I'd like us to be able to draw lessons from this. The first, which is already well established, is that when you're attacked it's no use burying your head in the sand. We've got to denounce and expose the lie or slander before it even materializes, drawing attention to why it's absurd.

The calibre of democratic debate and people's confidence are now indissociable from the architecture of the digital space and the ways it functions. The digital revolution doesn't just offer new information tools; it has changed the very way we get information. Search engines and social media have become not just a means of acquiring information but also filters; journalists no longer have a monopoly on information or control over how their content is broadcast; and searches carried out by members of the public are steered by algorithms which are likely to imprison them in "information silos".

We also have an obligation, as democratic societies, to ask questions about the economic model of collecting and exploiting personal data on social media, which is sold on to those pursuing a political agenda, as the scandal linked to Cambridge Analytica has just highlighted. In addition to the threat posed by authoritarian states is that posed by a "highest bidder", should he wish to influence the democratic process to his advantage.

RESPONSIBILITY OF DIGITAL PLATFORMS

So far, the major digital platforms have refused to take the phenomenon seriously. Yet we have to be clear: we wouldn't be seeing information manipulated as it is today without the existence of major digital platforms able to spread it on a massive scale and make it go viral.

Admittedly, the methods are the same as the ones the KGB used in the 1950s. Disinformation was already back then a pillar of the Soviet so-called "active measures" doctrine, which the security services conducted in order to influence the course of global events. You could say that, since the "Infektion" operation conducted by the KGB in 1983, which aimed at spreading the rumour that the American government had deliberately created the AIDS virus, things have simply moved to a new level. But there are spheres – such as that concerning information – in which the change of level is actually a change of nature. The striking power which social media allows, the ability to manage tens of thousands of accounts for practically nothing, paying a few disinformation soldiers, even using artificial intelligence, all enables hostile campaigns to be replicated ad infinitum, when it used to take years to mount them and increase the number of human contacts who were paid or acquired for the cause in other ways. An example of this is the recent Novichok nerve agent attack in Salisbury, which, right after the UK implicated Russia directly, saw an array of alternative explanations develop on the Internet in the space of a few hours, which were quickly spotted by private experts in detecting fake news.

So we can't go on doing nothing. I'd like us to take the following measures right away: firstly, demand transparency in the solutions which these platforms put in place, the impact and scope of which are too often difficult to assess. I understand that businesses protect the

intellectual property of their algorithms. I'd nevertheless like to know what goals they are pursuing, even generally, by employing these mathematical devices to develop their activities. I'm in favour of creating an obligation of transparency on individuals and companies which buy sponsored content of a political nature on a huge scale in order to promote the spread of it. The public relations exercises their leaders engage in aren't a response which is commensurate with the scale of the challenge. The statements of intent must be followed by concrete, measurable actions. Secondly, it's essential that personal data is subject to a much higher level of protection than exists today. Mechanisms guaranteeing the diversity and quality of information must also be put in place. We must together demand the highest level of protection and transparency for everyone. Thirdly, each platform must introduce a contact who can be reached and is responsible, making it possible to document and neutralize information-manipulation campaigns. This can be done in conjunction with the initiatives developed by civil society, such as the one presented by Christophe Deloire for Reporters Without Borders. To help mobilize those who could pretend to be unaware of who is genuinely responsible for disinformation and democratic disaffection, which is the end goal in this, I might add that the state will have to be able to publish, on its own initiative, sites on which it refuses to finance public adverts because of their extremist or conspiratorial nature.

During his speech presenting the national plan for the prevention of radicalization, the Prime Minister said that if platforms don't cooperate in the coming three months when it comes to removing illegal content, France will support in Brussels a European legislative initiative to force them to do so. France is also supporting Europol's finalization of the European database of illegal content.

As regards content to do with the manipulation of information, some of it may escape being categorized as such. So the current situation should prompt us to begin thinking about the essential standard-setting instruments to address the current unaccountability behind which these companies are hiding. I'm thinking in particular of the need to create a new status, besides that of content editor and web host, so that the responsibility of platforms in spreading manipulated information can be categorized as such.

EU ACTION

Action at European level is essential if there's to be a significant impact. France would therefore like to define with its partners a common set of European regulations, especially regarding the transparency of sponsored content, given the role they play in digital strategies to manipulate information. Platforms absolutely must fulfil a requirement to be honest with citizens. Of course, this set of regulations isn't incompatible with national initiatives which member states might wish to take.

We also have to create the right conditions for safeguarding pluralistic, high-quality information. I'm thinking, in particular, of recognition for neighbouring rights for newspaper publishers, as part of the reform of the Copyright Directive. Financial support mechanisms, at national and European level, could also be useful. In this respect, France believes that guidelines governing state aid shouldn't prevent newspaper companies from being supported or public broadcasting companies' online presence from being developed.

The European Commission took up the matter by bringing together in January a panel of experts comprising academics, journalists and representatives of digital platforms, which

issued its report on 12 March. It's a first step, but from where I stand it still doesn't set its sights high enough.

On the basis of this work and a public consultation, the Commission announced that a communication on this will be issued on 25 April 2018. We're waiting for this to be published, while hoping that the Commission will stress the need for a regulatory initiative on the transparency of sponsored content.

Finally, in cases where manipulated information is based on content which constitutes a criminal offence (hate speech, commercial scams, violations of intellectual property rights), we welcomed the guidelines, published by the Commission on 1 March 2018, on the removal of illegal content. These guidelines define operational measures aimed at more swiftly detecting and taking down illegal online content; strengthening cooperation between Internet platforms, trusted flaggers and law enforcement; and increasing transparency and safeguards for citizens.

COMBATING INTERFERENCE IN THE DEMOCRATIC PROCESS

Beyond European level, sharing experience and expertise with all our international partners is necessary; we must talk about this within the G7. This is precisely what I'll be doing in Toronto in a few weeks, with the G7 foreign and interior ministers. Canada, marking its G7 presidency, has in fact taken up the proposal we made last year to focus on the major issues linked to attempts to interfere in democratic processes. I'd like this meeting to provide an opportunity for a no-holds-barred discussion about this challenge and the solutions it calls for.

To this end, we've proposed that the G7 countries step up their coordination and capability to respond to these attempts to interfere by setting up, for example, a network of contacts allowing one or more partners to be alerted should an information manipulation campaign be detected, and information and solutions to be swiftly exchanged. We'd also like the G7 countries to agree on certain principles to be adhered to and standards promoted, especially in terms of transparent funding for political advertising and the strengthening of the media's and civil society's capabilities for detecting and combating manipulation when it occurs.

In this sphere which concerns the very principles of our democracy, public actors alone cannot provide a definitive solution. Civil societies, too, must develop antibodies so we can ensure we are collectively resilient.

They're already doing this. The participants in the afternoon's round tables have more than demonstrated this. In this respect, Reporters Without Borders' Journalism Trust Initiative has come up with an extremely interesting solution to give readers the means to exercise good judgment in the mass of information available today and distinguish between the work of professional journalists and what propaganda organs such as Russia Today or Sputnik produce. On a different note, I could also mention what Conspiracy Watch and the voluntary organization What the Fake – both supported by DILCRAH [French interministerial delegation for the fight against racism, anti-Semitism and anti-LGBT hatred] and the interministerial committee for preventing and detecting radicalization – are doing. The Council of Europe also held up France as an example for the *On te manipule* ["You're being manipulated"] campaign. So manipulation can be detected and denounced, and this effort

must be continued; it's then the responsibility of the media, particularly those such as the press agencies – and I welcome the participation in our discussions of the CEO of AFP, M. Emmanuel Hoog – which have a significant global impact, not to be involved in spreading these campaigns. Internet sites with the largest followings of young people also have a central responsibility.

Obviously media-education projects also play a decisive role. So we have a collective responsibility to give young people the essential critical instruments so that information online is used in an informed way.

The media-education plan announced by Françoise Nyssen, Minister of Culture, aims to meet this challenge. The world of research is also at work developing study programmes to give us a clearer understanding of the phenomenon and anticipate future threats. The European Union itself has a role to play, in this respect, in supporting what civil society is doing to combat disinformation and conspiracy theories on the Internet.

All these projects are concrete instruments of autonomy, giving everyone the possibility of finding their bearings in a chaotic, changing world of information. What's happening here is the formation of a citizen watchdog. I'd like my ministry to play its part in this and keep in touch with all these initiatives through our Digital Ambassador, David Martinon.

The emergence of a global digital space marks a break, the like of which has rarely existed in the history of mankind. No generation before us has been able to receive, in such a short period of time and from such varied horizons, as much information about world events. This unprecedented expansion of the public space certainly offers new opportunities when it comes to the aspirations which power our democracies; it also poses new risks of alienation for individuals and societies. Responding to these challenges is the task of our generation. We've contributed to this today. Thank you./.