Katarzyna Chałubińska-Jentkiewicz*

„Other devils were active there”.

Kornel Ujejski, *Z dymem pożarów*
(With the Smoke of Fires), 1846

Disinformation – and what else?

Abstract

The fundamental element of safety and of the presence of a sense of security is their being communicated to the public, which precedes development based on common perceptions and interpretations of the surrounding reality. With the development of societies, the progress of digitalisation in the field of communication, and the smooth transmission of information and data, the individualisation and specialisation of communications leading to completely new forms of activity, and social media and messages which are not addressed to the public, have become increasingly important. This refers to all events and phenomena in the public sphere, and its impact on civic life, the manner of its assessment, and the narrative which arises, and which is considered to be true by certain social groups or societies, as they can identify themselves with it, and, finally, treat it as their own – post truth.

Key words: disinformation, digitalisation, communication

[*] Katarzyna Chałubińska-Jentkiewicz, Ph.D. hab. of legal sciences, associate professor and head of the Department of Cyber Security Law and New Technologies at the Institute of Law War Studies Academy in Warsaw, director of the Academic Center for Cybersecurity Policy, e-mail: kasiachalubinska@gmail.com.

Introduction

It can be said that the role of the media in defining security issues is linked to the social dimension of defining, identifying, and neutralising threats. Extending the sphere of the security of the State and its citizens to the virtual environment, and the reference to cybersecurity, are natural consequences of the development of communication technologies and related social phenomena centred on the acquisition, processing, and distribution of information. Such a process usually leads to amendments to specific laws, which are intended to adapt to the legal environment, and define new social-activity rules in the domain of security, and thus reduce the level of threat. The media are transforming, and it is becoming increasingly difficult to define them.

Media and security

Due to the predominance of the Internet and digital forms of information, the traditional media such as press, radio, and television have been extended to include news and social-media sites, blogs, and video-upload platforms which allow the simultaneous exchange of opinions, feelings, and observations, i.e. information. These new formats are not as institutionalised as the traditional media (which are regulated by way of licensing and registration procedures). The Internet has become a place to create own information spaces, being at the same time a new form of medium, and a new public sphere which does not know territorial, language, or national boundaries. This dimension of the often uncontrolled expansion of the media space requires a new regulatory approach in terms of security methods and techniques. New forms of threats resulting from malware, identity theft on the Internet, impersonating official websites, or *phishing*, give rise to completely new social-engineering techniques which are applied to obtain information, including illegally, to create new situations which favour specific interest groups, including State players in the context of international relations. The armed forces of individual States are beginning to organise units for the protection of cyberspace – especially in relation to established State-security institutions and other spheres of public safety which affect the daily lives of citizens. The media of our interest are, indeed, those related to the broadly defined domain of State security. In the sphere of cyberspace, so-called social-engineering attacks will be discussed. Social-engineering techniques themselves, and the general mechanisms for defining security issues, directly relate to a theoretical dictum called constructivism (also known as constructionism).

On one hand, there are radical statements about the annihilation/simulacrisation of reality, and its implosion within the media; on the other hand, the conviction that we have entered into a new epistemological paradigm – a new form of knowledge - and a new form of culture, known as cyberculture, or, more broadly, technological culture[1]. Journalists themselves are also contributing to the sense of unreality. Pierre Bourdieu, in his lectures entitled *About television. The rule of journalism*, draws attention to the opportunism of journalists, i.e. their tendency to be dependent on advertisers, and the opinion of their audience. „Journalism, like politics and economics, and much more than science, art, literature or law, is constantly being tested for market judgments, whether through direct (customer) or indirect (audience) sanctions”[2].

Sociology stresses the importance of W.I. Thomas's Theorem – „if men define situations as real, they are real in their consequences”[3]. In the sphere of security, if a threat is misidentified from the outset, e.g. under the influence of different presumptions, and taking speculation as facts, then the measures taken, having a specific objective dimension, are not adapted to the real threat. If fatal incidents occur, such as construction disasters, car accidents, or mass murders by mentally ill people, then the journalist's first question or hypothesis generally implies the possibility of a terrorist attack[4]. It should be stressed that the definition of security is a continuous process, and refers to specific public-security contexts. It is never the case that a described and defined safety issue is established once and for all. The perception of security problems is very dynamic, and subject to comprehensive processes in which the media only deal with a certain dimension – that of social communication.

[1] M. Lisowska-Magdziarz, *Metodologia badań nad mediami – nurty, kierunki, koncepcje, nowe wyzwania*, „Studia Medioznawcze” 2013, nr 2, s. 38.

[2] P. Bourdieu, *O telewizji. Panowanie dziennikarstwa*, Warszawa 2011, s. 107.

[3] R.K. Merton, *Samospełniające się proroctwo* [w:] *Socjologia. Lektury*, red. P. Sztompka, M. Kucia, Kraków 2006, s. 361.

[4] M. Ciesielski, *Terroryzm i media w kontekście paniki moralnej*, „Kwartalnik Bellona” 2012, nr 2, s. 176–177.

Social media

Social media, especially when open, in which all users have the opportunity to post their own content, so is practically out of the administrators' control, or is controlled selectively and insufficiently, constitute a new type of threat, unknown before the advent of the Internet. Such open social media can serve not only to exchange data (opinions, assessments, thoughts, assumptions, interpretations, etc.) within small local communities, but can easily have a global reach. It can be exemplified by the activities of famous figures – actors, artists, businessmen, and increasingly often politicians – who, on the one hand, can promote specific products in this way and draw profit from advertising campaigns, but, on the other hand, can spread their own ideas, beliefs, thoughts, interpretations, and theories. An important point is that the fine line between facts and opinions, conclusions, and evaluations is blurred in the mass media, and especially in the open social media (such as Facebook, Instagram, Twitter, YouTube, and VKontakte).

Because social media publish content related to all spheres of social life, and disseminate it in real time, it has become an area of the organised activity of interest groups which can threaten national security. In crisis situations involving sudden events and threats to society as a whole, the media often have difficulty in choosing the right means of communication – whether it comes to language or form. On a daily basis, in the pursuit of sensational news, often unimportant issues and problems, which are not very significant, are elevated to the rank of major events of great seriousness for every citizen. The reason for this is that the greatest interest is in safety issues, because they can, by definition, affect all of us. Consequently, if a real threat emerges later, when the danger can be still minimised, or at least limited for reasons such as an effective security policy, the media broadcasts are not always adequately received – they are perceived as dubious by citizens. The public (or part of it) presumes that this is just more fake news, or a falsely generated account of a threat, aimed at improving the readership, audience, statistics, or website hits.

The media as an instrument of disinformation

A state of widespread danger, which affects the whole of society, and requires exceptional countermeasures to be taken, and involving a large part of the attention and commitment of those in power, is a circumstance creating favourable conditions for disinformation.

The problem with modern media is that we do not know how to define modernity and media in general. According to Leszek Kołakowski, „Without knowing what 'modernity' is, we have recently been trying to move forward from our question and talk about 'post-modernity' (this is an extension or imitation of slightly older expressions, such as 'post-industrial society', 'post-capitalism', etc.). I do not know what 'post-modernity' is and how it differs from 'pre-modernity', nor do I have the impression that I should know. And what can come after 'post-modernity'? Post-post-modernity, neo-post-modernity, neo-anti-modernity?"[5].

Among multiple elements which can define this new order, it is worth noting at this point several distinctive features of contemporary perceptions of the world through the prism of the media. Thanks to the media, we can feel both local and global. We are relying more and more on media descriptions than on our real experiences. We are able to question any authority, including scientists, because the media constantly provide us with arguments for and against every statement. Since the creation and proliferation of the Internet, we have been living in a different reality.

Anthony Giddens maintains that we live in the late-modern age, and that means that we have one foot permanently in the local environment, but the other in the global world. „Although we all live in local environments, the worlds experienced by most of us are truly global"[6]. Manuel Castells confirmed this assertion, looking at it from the other, global, perspective. „The social structure is global, but most of human experience is local, in both territorial and cultural terms"[7]. Zygmunt Bauman perceived globalisation as a reduction in distance in many respects. „This incredible sense of 'filling the world' is commonly referred to as 'globalisation.' With transmission speeds reaching limit values – comparable to the speed of light – (including action triggers), the almost-simultaneous sequence of cause and effect reduces even the greatest distances, and ultimately invalidates the distinction between cause and effect

[5] L. Kołakowski, *Cywilizacja na ławie oskarżonych*, Warszawa 1990, s. 201.

[6] A. Giddens, *Nowoczesność i tożsamość. „Ja" i społeczeństwo w epoce późnej nowoczesności*, Warszawa 2012, s. 251.

[7] M. Castells, *Communication Power*, Warszawa 2013, s. 38.

itself. Despite all practical intentions and goals, we all live today in a close, even intimate, neighbourhood”[8].

So we are somewhere between what is local to us and what is global to all of us. Sometimes we feel more local, and sometimes we take a global perspective. This is, according to Giddens, our dialectic of the local and global, or „interplay between participation in local contexts and global trends”[9].

The natural environment for disinformational activities is the information chaos and the emotional nature of media releases, in which various interest groups often clash. If we are dealing with the dynamic developments of a situation and the unpredictability of social processes, it is very difficult, or even impossible in practice, to distinguish the activities of ordinary public figures, including experts, advisors, clergymen, or scientists commenting on a given threat, from deliberate actions inspired by foreign special services or other State players.

Both in disinformation and influence, „the goal is perceived as an accomplice”[10]. In the author’s opinion, it is enough to instil even a minimal but adequate catalyst into public opinion, and the social reaction which will follow will be in line with the expectations of the disinforming parties, with the semblance of spontaneity. It is emphasised that misleading is a technique, while disinformation is a doctrine[11].

Disinformation – what can be done about it?

Disinformation undermines democracy because democracy depends on the free flow of information. It is an attack on the very heart of our democracy. I am not talking about information or news which is simply wrong or inaccurate. The essence of disinformation is information or news which is deliberately false in order to manipulate and mislead people. Part of the problem is that there is no agreed-on terminology to describe it.

Disinformation – the deliberate creation and distribution of information which is false and deceptive in order to mislead an audience. Information which you dislike or disagree with is often called fake news. For example, the Russians

[8] Z. Bauman, *Społeczeństwo w stanie oblężenia*, Warszawa 2007, s. 18.
[9] A. Giddens, op. cit.
[10] Z. Bauman, op. cit., s. 18.
[11] Ibidem, s. 11.

were calling Western media fake news long before Donald Trump did. This disinformation is a felony, a mixture of truth and falsity. The Russian are masters of having a kernel of truth in their disinformation. That is in part why it is so effective and hard to fight.

Misinformation – information which is false, though not always deliberately so, being created intentionally, inadvertently or by mistake.

Propaganda – information which might or might not be true, which is designed to engender support for a political view or an ideology. This is also a tricky term. It seems to be morally neutral. Propaganda as a word has different implications. Advertising is a form of propaganda. What the United States Information Agency did during the Cold War was defined as propaganda. This is, strictly, a misdemeanour. But it often uses content which is true.

There are no easy answers to the problem of disinformation. Democracies are not very good at fighting disinformation. The value placed on free speech and debate is our problem, and our constitutions and laws are focused on protecting the freedom of speech, notwithstanding whether the message is true or false. We still believe that truth will win out. Probably we need to look at the circumstances of hate speech, and to borrow some solutions in the new digital area of disinformation.

Information wars – tools

There are the exact same tools – e.g. behavioural-data analysis, audience segmentation, programmatic ad buying, etc. – as used in effective advertising campaigns.

The Internet Research Agency in St. Petersburg uses the same behavioural data and machine –learning algorithms as Coca Cola and Nike. Content created by the Internet Research Agency in St. Petersburg reached 126 million people on Facebook, and more than 20 million on Instagram. They created a website called Black Matters US, and promoted it with ads and content on Facebook, Google+, Instagram, and Twitter. In February 2016 the site had 100,000 subscribers. They created other entities and sites like Blacktivist and Black Guns Matter to both promote Black Matters US, and increase their total number of African-American followers.

If you want to know about these new tools in the future, you should look at new tools in future advertising.

All the big platforms depend on the harvesting and use of personal information. Our data is the currency of the digital economy, because such platforms as Google, Facebook, Amazon, Microsoft, and Apple depend on data and personal information. In Europe people own their own information according to the rule of the information autonomy (the famous GDPR – the EU's General Data Protection Regulation). The principle is simple: people want to know everything about their data, and they need to control what information is being collected about them, how it is collected, and how it is used.

Law – and what else?

According to the European Parliament Resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes (2019/2810(RSP)), the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions Tackling online disinformation: a European Approach (COM/2018/236 final), 83% of Europeans considered fake news to present a problem for democracy in general, either „definitely" (45%) or „to some extent" (38%). Intentional disinformation aimed at influencing elections and immigration policies were the top-two categories considered likely to cause harm to society, according to the respondents to a public consultation conducted by the Commission. These were closely followed by disinformation in the fields of health, environment, and security policies. One consequence was the Code of Practice on Disinformation.

Some online platforms acted swiftly and effectively to protect users from disinformation; the Code of Practice was signed by the online platforms Facebook, Google, Twitter, and Mozilla, as well as by advertisers and the advertising industry, in October 2018, and set self-regulatory standards to fight disinformation. The Code aimed at achieving the objectives set out by the April 2018 Commission Communication on tackling online disinformation (COM/2018/236 final of 26.4.2018) by prescribing a wide range of commitments, from transparency in political advertising to the closure of fake accounts and the demonetisation of purveyors of disinformation.

According to the Communication from the Commission to the European Parliament, the European Council, and the Council's Nineteenth Progress Report towards an effective and genuine Security Union (COM/2019/353 final), protecting democratic processes and institutions from disinformation and related interference is a major challenge for societies across the globe. To tackle this, the EU has put in place a robust framework for coordinated action against disinformation, with full respect for European values and fundamental rights. As set out in the Joint Communication of 14 June 2019 on the implementation of the Action Plan against Disinformation, the work on several complementary strands has helped to close down the space for disinformation and preserve the integrity of the European Parliament elections.

In the Communications Decency Act (CDA) in section 230 it is stated – no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provide by another information content provider. This means that all gigantic platforms blanket immunity from any liability for their content. The Russians became experts at using two parts of Facebook's advertising infrastructures – the ads auction and something called Custom Audiences.

At the same time, it should be stressed that the system of Polish penal law is not adapted to prosecuting this type of activity, because of the inadequate narrowing of the scope of the offence of disinformation. Apart from the fact that the definition of disinformation in penal law has been limited to misleading Polish State authorities, it must still be linked to the provision of intelligence services to the Republic of Poland (intelligence disinformation). The *actus reus (physical)* component of the offence of disinformation, as described in Article 132 of the Penal Code[12], does not in any way take into account the intentional influence of the media on public opinion and the State authority[13].

„Whoever, by providing intelligence services to the Republic of Poland, deceives a Polish State authority by supplying forged or falsified documents or other objects, or by concealing true information, or providing false information of significant importance to the Republic of Poland, is punishable by imprisonment of between one and 10 years"[14].

[12] The Penal Code of 6 June 1997, Journal of Laws of 1997, no. 88, item 553; consolidated text, Journal of Laws of 2019, item 1950.

[13] „Whoever, by providing intelligence services to the Republic of Poland, deceives a Polish State authority by providing forged or falsified documents or other objects, or by concealing true information, or by providing false information of significant importance to the Republic of Poland, is punishable by imprisonment of between one and 10 years" – ibidem, article 132.

[14] Ibidem.

The basic aim of disinformation is precisely to influence groups which are key to the organisation of social life and the security policy of the State. Strategic groups mean social groups which are of particular strategic or tactical importance to so-called destabilisation agents. This is not about paralysing or breaking up such groups, but about inspiring, organising and structuring them[15] – generally in terms of their interaction with those in power. The objective here is to fuel and exploit the collective sentiments or needs (including ideologies) of key groups. Moreover, such groups can stir up anger, resentment and disappointment, for example, related to the nature of steps taken by the Government to deal with the threat. The media, instead of being a filter, are a catalyst for social unrest, and it is becoming difficult to assess whether they are provoked by interest groups, or they are an expression of civic opposition and rebellion against threats and the security policy being implemented. If, in a crisis situation created by a threat to the security of the State and its citizens, there is a confrontation between specific social groups, especially those organised around the political system of the State, then not only the security policy being pursued can lose its legitimacy, but the confrontation can affect lower social areas covering entire sectors of society and lead to real social unrest.

Bibliography

Bauman Z., *Społeczeństwo w stanie oblężenia*, Warszawa 2007.

Bourdieu P., *O telewizji. Panowanie dziennikarstwa*, Warszawa 2011.

Castells M., *Communication Power*, Warszawa 2013.

Ciesielski M., *Terroryzm i media w kontekście paniki moralnej*, „Kwartalnik Bellona" 2012, nr 2.

Giddens A., *Nowoczesność i tożsamość. „Ja" i społeczeństwo w epoce późnej nowoczesności*, Warszawa 2012.

Kołakowski L., *Cywilizacja na ławie oskarżonych*, Warszawa 1990.

Lisowska-Magdziarz M., *Metodologia badań nad mediami – nurty, kierunki, koncepcje, nowe wyzwania*, „Studia Medioznawcze" 2013, nr 2.

Merton R.K., *Samospełniające się proroctwo* [w:] *Socjologia. Lektury*, red. P. Sztompka, M. Kucia, Kraków 2006.

Mucchielli R., *La Subversion* [w:] V. Volkoff, *Psychosocjotechnika, dezinformacja – oręż wojny*, Komorów 1999.

[15] See R. Mucchielli, *La Subversion* [w:] V. Volkoff, *Psychosocjotechnika, dezinformacja – oręż wojny*, Komorów 1999, s. 111–115.

Dezinformacja – i co jeszcze?

Streszczenie

Podstawowym elementem zarówno bezpieczeństwa, jak i braku poczucia niepewności jest informowanie o nich społeczeństwa, co poprzedza rozwój oparty o wspólne wyobrażenia i interpretację otaczającej rzeczywistości. Wraz z rozwojem społeczeństwa, postępem cyfryzacji w sferze komunikacji oraz łatwością przekazywania informacji i danych coraz większego znaczenia nabiera kwestia zindywidualizowanego i wyspecjalizowanego przekazu prowadząca do zupełnie nowych form aktywności, a także media społecznościowe i przekaz, który nie jest skierowany do ogółu społeczeństwa. Dotyczy to wszelkich wydarzeń i zjawisk zachodzących w sferze publicznej, ich oddziaływania na tę sferę oraz sposobu oceny, a także narracji budowanej i uznawanej za wiarygodną przez określone grupy społeczne czy społeczności, z którą mogą się one utożsamiać, a w końcu traktować jak własną – postprawdę.

Słowa kluczowe: dezinformacja, cyfryzacja, komunikacja