

LEGAL AND INSTITUTIONAL ACTIVITIES OF EU MEMBER STATES TO COUNTERACT FALSE NEWS AND DISINFORMATION

Milan Miljković, PhD ¹

Goran Matić, PhD

Ivana Rebrača, MA

Office of the National Security Council and Classified Information
Protection of the Government of the Republic of Serbia

Abstract: Since the ancient times information has been used for manipulative purposes, and also as a means for carrying on conflicts. In the modern information age information space has only been given an added topicality, as a battlespace of today's global society. This added topicality also applies to the use of disinformation and fake news within the concept of "hybrid and information warfare" as a way of waging geopolitical conflicts between the great powers. Social media and online platforms play an important role in accelerating the spread of fake news because they enable its global reach. For that reason, modern states are confronted with a problem of ensuring an efficient control and protection of the national information sphere, and, by the same token, national security. The mentioned issue ranks high on the security agenda of European legislators due to the fact that the European Parliament election will be held in 2019. In this connection, an EU-wide campaign against fake news in the field of legislation is being conducted by the governments of many European countries. Bearing in mind the above-mentioned, counteracting fake news and disinformation can be considered from the two aspects, namely: 1) from the aspect of defense and protection of national security, and 2) protection of the electoral political process. On the legal level, at the end of 2016, the European Parliament passed a resolution on EU strategic communication to counteract propaganda against it by third parties. European Commission presented at the end of 2018 an Action Plan against Disinformation setting out additional steps against disinformation. On the institutional level, the Task Force East Stratcom was set up in 2015 within the European Service for External Action. So far the team made up of 16 staff members, recruited from the EU institutions or seconded by EU Member States, has documented, analysed and published over 4,500 examples of disinformation and has thus contributed to understanding tools, tactics, techniques and intentions of disinformation disseminated by foreign sources.

Keywords: disinformation, fake news, social media

¹ milanmiljkovic04011@gmail.com

INTRODUCTION

Owing to the massive use of information technology in the area of communications, modern states are confronted with a problem of ensuring efficient control and protection of their national information sphere, and by the same token, national security. Since the ancient times, information has been used for manipulative purposes, and as a means for carrying on conflicts. In the modern information age information space has only been given an added topicality, as a battlespace of today's global society. This added topicality also applies to the use of disinformation and fake news within the concept of "hybrid and information warfare", as a way of waging geopolitical conflicts between the great powers.

From the aspect of protecting internal security and political stability, the use of propaganda and disinformation in the context of "information operations" by an external factor is classified as a type of subversive activities that, as such, can be divided into the following: 1) political influence operations, 2) media and public opinion influence operations, and 3) ideological- political indoctrination (Miljković, 2016:206).

Fake news poses a significant security problem to the present day society, as indicated in an EU survey conducted in February 2018 by interviewing over 25,576 respondents in 28 member states, on which occasion 85% citizens have identified fake news as a problem in their countries.² The foregoing issue ranks high on the security agenda of European legislators due to the fact that the European Parliament election will be held in 2019. In this connection, an EU-wide campaign against fake news in the field of legislation is being conducted by the governments of many European countries. Germany and France have already introduced and implemented, respectively regulations aimed at removing or blocking hate speech and untrue contents on online communications platforms. The Great Britain is planning to designate a unit within its security apparatus to counteract the above threats. The Czech Republic has already set up such a body within its Ministry of Interior to counteract hybrid threats and disinformation, to mention just a few examples.

DEFINITIONS OF TERMS AND KEY FEATURES OF DISINFORMATION AND FAKE NEWS

The term disinformation, as defined by the High level Group on fake news and online disinformation, includes all forms of false, inaccurate or misleading information designed, presented and promoted to intentionally cause public harm or for profit.³ Disinformation, i.e. provably false or misleading information, fabricat-

² Final results of the Eurobarometer on fake news and online disinformation, <https://ec.europa.eu/digital-single-market/en/news/final-results-eurobarometer-fake-news-and-online-disinformation>

³ Report of the independent High level Group on fake news and online disinformation, <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news->

ed, presented and disseminated in order to gain an economic profit or purposefully mislead the public is harmful to the public debate; it undermines citizens' trust in institutions and media, and weakens a country's internal stability and its democratic processes, such as electoral processes. Therefore, the goal of information manipulation is not to persuade people to accept any alternative political ideology, but to bring about a weakening of the existing internal stability of a country.

That broad definition also covers partly the term "fake news", which has been put into the political context by most of the public and experts over that past few years. In this regard, fake news is, in fact, a considerably narrower term than the concept of disinformation. As defined by experts, false news is a deliberate or conscious online presentation of false claims as news (Gelfert, 2018: 97). The term also implies "news with no factual grounds, that is nonetheless presented as news" (Hunt, 2017: 4). The goal of fake news grounded on non-existing or distorted "facts" is to mislead and manipulate the public opinion.

Human behaviour on social networks is a key factor in spreading fake news, along with the fact that social media have almost replaced traditional media. A growing number of EU citizens (46% on average in 2016) follow news on social networks; six out of ten news articles shared are passed on without being read first.⁴ The findings of a survey show that fake information is shared more than true information, and that false stories get more attention, and are therefore distributed at a greater speed.⁵ According to the survey conclusions, true news is very rarely spread to more than 1,000 individuals. On the other hand, 1% of the most popular fake news usually reaches 1,000 to 100,000 people. Moreover, it takes six times longer for true information to reach 1,500 people in comparison with false news.

Crisis situations, such as natural disasters, bomb attacks or armed assaults, are fake news authors' favourites; they draw on people's emotions surrounding such events in an attempt to produce maximum reverberations for their creations. The authors of a study inspired by a circulation of numerous rumours after the 2013 Boston marathon, claim that political fake news spreads at the fastest rate, well ahead "urban legends" and economy news. The "terrorism and war" news category is ranked fourth, whereas natural disasters news is placed at the bottom of the list.

In addition to malicious intentions, confusion and bustle that follow in the wake of emergencies may contribute to the appearance of fake news due to the lack of time to verify information with traditional media, or owing to errors of official sources.

and-online-disinformation

⁴ Lažne vesti i odgovor EU, . <https://europa.rs>,

⁵ A study by the prestigious Massachusetts Institute of Technology published in *Science*, March 2019 claims that fake news spreads much faster on social networks than true news, regardless of its subject.

POLITICAL AND SECURITY-RELATED SIGNIFICANCE AND CLASSIFICATION OF SPREADING FAKE NEWS AND DISINFORMATION

The fake news issue, as a salient challenge to states' internal security is linked to the fact that social media and online platforms, which represent an important source of information nowadays, play an important role in accelerating the spread of fake news, and enable their global dissemination and reach, thus also accelerating the spread of internal instability of a country. Moreover, that issue is compounded by a rapid spread of massive quantities of false information, which may cause considerably adverse and manipulative effects on the public opinion and therefore become a major security problem of today. (Lohr, 2018).⁶

The political and security-related significance of spreading fake news can be determined on the basis of various criteria. National authors point out that if the extent of harm is used as a classification criterion, it will produce a differentiation between *national and international political implications*. At the same time, they suggest that such a classification is essentially relativised by the very fact that global communication networks make it possible for fake news to be available across the whole globe within a very short period of time.

Further to the above mentioned, if fake news is classified according to the source of dissemination, it can be divided into fake news coming from individuals, political parties, interest groups or intelligence services of some states.

Moreover, when classification proceeds from the criterion of target object, fake news is divided into that aimed at a particular politician, collectivity, political party or state.

All the above-mentioned criteria are relevant while examining the reach of fake news in relation to the target of its dissemination. However, the objective of every pseudo-news item is to effectuate a propaganda activity, as a planned and designed dissemination of political ideas and attitudes for the purpose of exerting influence on the cognition and behaviour of both individual and collectivity. Detecting the ultimate goal, as something that steers the process of disseminating fake news, considerably determines the character and importance of political implications, and then, in the context of threat it can be qualified as risks from secessionist strivings, armed rebellion, terrorism, national and religious extremism, intelligence activities, preparation of a political assassination, so-called "colour revolutions", etc. (Bodrožić, 2017: 253).

Having in mind the above-stated, counteracting fake news and disinformation can be considered from the two aspects, namely: 1) from the aspect of de-

⁶ Lohr, S. (2018). "It's True: False News Spreads Faster and Wider. And Humans Are to Blame". The New York Times. <https://www.nytimes.com/2018/03/08/technology/twitter-fake-newsresearch.html>, see also: Vosoughi, S., Roy, D., and Aral, S. (2018). "The spread of true and false news online". Science, 359(6380), 1146-1151. <http://science.sciencemag.org/content/359/6380/1146>.

fense and protection of national security – when it is classified as an element of the information and hybrid warfare concept, and 2) protection of the electoral political process.

USE OF FAKE NEWS AND DISINFORMATION WITHIN THE CONTEXT OF INFORMATION AND HYBRID WARFARE

The news in general, and fake news, as its subcategory, carried by modern technological means, enabling its fast and inexpensive broadcasting, are emerging as a generator of political, moral and other attitudes of individuals and societies, and by the same token, drivers of internal political events in a country (Bodrožić, 2017: 251).

Sometimes the goal of fake news is merely to increase the network traffic (clickbait). However, when it is used for the purpose of political deception or deception for the purpose of international relations, it falls into the category of disinformation, as a strategic tool for undermining internal stability and, by the same token, national security of an external adversary.

Fake news is considered as a part of subversive activity, specifically as a component of information warfare, that is to say as an instrument of information operations aimed at producing information effect on an adversary's internal stability either in the context of a doctrine of crisis causation or crisis management, and, in a broader sense, public opinion management, citizen discontent and riot causation, thus covertly imposing one's own interests, or it is regarded in the context of influencing national and world public opinions in such a manner so as to create conditions for a media warfare to develop into a real war (*Stajić, Gaćinović, 2007: 242*).

Military experts' assessments of an increasingly diminishing borderline between war and peace in the modern age also point to the topicality of fake news as an information weapon in contemporary conflicts, and to the fact that "the methods of conflict being used are changing toward the all-inclusive employment of other non-military measures." (Gerasimov, 2017). The foregoing statement by General Gerasimov, the current Chief of the Russian Federation Armed Forces General Staff is quoted by many modern security and military theoreticians with the intention of stressing the significance of fake news as a technique of information operations in contemporary conflicts, i.e. hybrid warfare.

Information operations (IO) have been defined by civil experts in the subject area, as well as in doctrinal documents of the Western countries' armed forces. According to the U.S. authors, information warfare covers 1) a striving to learn everything about an adversary, and to prevent an adversary from learning much about you; 2) turning "the balance of information and knowledge" to one's advantage, especially if there is no balance of power; 3) using knowledge in such a manner, so as to enable small capital and labour to increase (Arquilla, Ron-

feldt, 2017). The following definition of the term offered by Richard Szafranski is regarded as the most complete and acceptable one: "information warfare is a hostile activity directed against any part of the knowledge and belief systems of an adversary". Regardless of whether or not it is conducted against an external adversary or internal groups, the ultimate goal of information warfare is using information warfare for bringing about a change (influence, manipulation, attack) to the knowledge and belief system of an external adversary.

So far several Russian authors have defined information warfare and information operations. The Russian expert S.P. Rastorguyev discussed the concept of information warfare in his book *An Introduction to the Formal Theory of Information Warfare* published in 2003. He defines information warfare "as a battle between states involving the use of exclusively information weapons in the sphere of information models". The ultimate goal to be achieved is to gain knowledge of a specific information system, and to subsequently use such knowledge purposefully in order to distort or destroy the model of an adversary's world (environment). He argues that an information weapon can be a technical, biological, or social instrument used for purposeful production, transmission, presentation or blocking of data and processes connected to a database. (Rastorguyev, 2003: p. 6,7).

Similarly, hybrid warfare consists of different elements of conventional and non-conventional capabilities, political and economic activities, information activities, irregular tactics and formations, terrorist acts, including indiscriminate violence and coercion, and criminal disorder (Hoffman, 2007). The use of information activities for achieving political and military goals in a conflict has increased, and in many cases it has exceeded the power of weapons in its effectiveness (Gerasimov, 2013). "The soft dimension" of information operations, i.e. its information-perceptive aspect (propaganda, deception and disinformation) demand much less financial means, which opens up possibilities for using disinformation and fake news as hybrid weapons (Miljković, 2017: 169-180).

In this regard, it can be concluded that the use of fake news and disinformation represents one of the techniques for conducting information and hybrid warfare in times of peace and war alike which is undertaken to undermine an adversary's internal stability and its citizens' confidence in their own military and state leaderships and institutions. The use of fake news has notably gained importance due to the fact that a significant part of the contemporary population gets informed through modern mobile communication devices and social networks disseminating information that has not been subjected to any control of the state authorities so far.

EU'S EXPERIENCE WITH REGARD TO COUNTERING "FAKE NEWS" FROM THE ASPECT OF DEFENCE AND PROTECTION FROM HYBRID AND INFORMATION WARFARE

Fake news and disinformation are identified as significant security threats in national security strategies of many EU countries. Along these lines, the Czech Republic and Poland consider hybrid threats and fake news "as significant challenges to the national security and defence". Their security experts hold a view that "a hybrid" war incorporates spreading fake news for the purpose of changing public attitudes.

The Security Strategy of the Czech Republic 2015 states that "threats to the security of allies may be of the classical military nature or they make take the vague form of hybrid warfare." In this connection, the above Security Strategy identifies threats that can bring about "the weakening of the cooperative security mechanism and of political and international legal commitments in the area of security ", and claims that some states seek to achieve a revision of the existing international order and are ready to pursue their power-seeking goals through hybrid warfare combining conventional and non-conventional military means with non-military tools (propaganda using traditional and new media, disinformation intelligence operations, cyber attacks, political and economic pressure, and deployment of unmarked military personnel).⁷

On the legal level, the Czech legislation does not formally recognise the concept of "disinformation" or "propaganda" from the aspect of criminal law, and consequently there is no definition of factual circumstances of "disinformation-" or "propaganda-based" crime. It follows from the above that fake news and disinformation are, first and foremost, brought into relationship with criminal offences concerning terrorism and counteracting foreign intelligence services' impact on internal developments in the country. In this regard, as stated in the Czech Ministry of Interior's reports, disinformation campaigns are divided into three groups: 1) terrorism-related disinformation campaign - aimed at inciting and provoking individuals to solve their problems by transforming themselves into followers of the fundamentalist ideology; 2) extremism-related disinformation campaign - aimed at inciting and provoking society to crimes connected to extremism and actions in contravention of democratic and constitutional principles, and 3) pro-Kremlin disinformation campaign - aimed at provoking undemocratic and extremist attitudes, and causing a feeling of helplessness in a democratic system by using lies and half-thruths, relativising facts, and manipulating society.⁸ In view of the above-mentioned, the task of countering fake news, disinformation and hybrid threats on the institutional level in the Czech Republic is entrusted to its Ministry of Interior. To that end, it set up the Centre against Terrorism and hybrid threats in 2017.⁹

Similarly, the fight against fake news in Poland is most noticeable in the form of counteracting activities of foreign intelligence services towards its population, or neutralising Russian hybrid warfare networks operating in Poland and inspiring its citizens to take targeted subversive activities against their own country in the interest of the Russian Federation, as stated by representatives of Polish security services. Namely, in May 2018 the Polish Intelligence Service (ABW) released a press statement on the arrest of a female Russian national on Polish soil on suspicion of instigating tensions with Ukraine in collaboration with her associates.¹⁰

The issue of countering fake news was given an extra topicality in France from the aspect of protecting national interests during 2017, the year of the presidential election, which was won by Emmanuel Macron eventually. At the beginning of 2018, President Macron stressed that CSA (French Media Regulatory Authority) should provide necessary capacities and a legal framework to effectively counter attempts made by television channels controlled by foreign states to destabilise the internal situation in France. Such an initiative was justified by a need to protect democratic institutions from any regime propagating “political non-liberalism.” Owing to that, following the adoption of a Fake News Act at the end of 2018 the Broadcasting Council was given a power to prevent, suspend or stop programs broadcast by television channels “controlled by a foreign state or under the influence of that foreign state”, if they have a harmful impact on France’s fundamental interests.¹¹

EU’S EXPERIENCE IN COUNTERING “FAKE NEWS” FROM THE ASPECT OF PROTECTING ELECTORAL PROCESS BY CRIMINAL LAW

Earlier periods of societal development have also been characterized by dissemination of fake news, particularly in the times of obvious conflicts. Nowadays, online media stand for what the printed press, radio and television used to be. The increase in audiences and quantity of distributed messages has not, however, brought about an increase in the quality of information; instead, both traditional means of public information and new communication technologies are emerging (when observed in conjunction) as powerful mechanisms of political activity, particularly during the period of conducting an electoral process (Parezanović, 2013: 324-337).

When considering challenges in countering fake news in the electoral process from the aspect of criminal law, it should be underlined that fake news is not, in most cases, illegal information, i.e. statements incriminated by criminal laws, such as defamations or posted contents inciting racial hatred. In addition,

¹⁰ Poland busts Russian ‘hybrid warfare’ ring, <https://www.dw.com/en/poland-busts-russian-hybrid-warfare-ring/a-43831566>

¹¹ France passes controversial ‘fake news’ law, <https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law>

fake news most often represents neither a satire nor a journalistic error, to which corrective policies are applied. The focus in this case is on countering deliberate disinformation, whether it be politically or commercially motivated. For that reason, countering fake news poses a challenge to any acting judge with no power to simply put a ban on it. This happens mainly due to the speed at which fabricated news spreads through social media and other digital platforms. Furthermore, it is very hard to establish the “real truth” about such issues in every particular case, given that any undue interference by a court of law would be perceived as an act of censorship and abrogation of the freedom of speech.

Shortly before holding the Federal Elections in Germany in September 2017, the Bundestag adopted an Act to Improve Enforcement of the Law in Social Networks, commonly known as *NetzDG*. It prescribes that social media platforms (Facebook, Twitter and Youtube) be sanctioned with regulatory fines of up to 5 million euros, if they fail to remove fake news and hate speech within 24 hours from issuing a regulatory fine order. The monetary penalties shall be imposed on the foregoing and similar online platforms if they fail to respond efficiently enough to an unlawful content. The German authorities introduced such a legal solution in an effort to regulate activities of the social network management companies, force them to label a disputable content, and remove it from their websites, if it turns out that it is about child pornography, instigation to terrorism, hate crimes, and also so-called fake news. In addition, *NetzDG* stipulates individual responsibility, so that managers of the companies in question run the risk of being ordered to pay fines of up to 5 million euros, if they fail to comply with the *NetzDG*'s provisions.

Along these lines, at the end of 2018 the French Parliament endorsed two laws against fake news and information manipulation during the electoral period, the passage of which was supported by president Macron himself. Those laws should enable a candidate or political party to complain to the court and demand an urgent suspension of fake news dissemination during a three-month period prior to a national election. Those legal acts also aim at achieving a stronger transparency of online platforms, such as Facebook and Twitter in the course of disseminating a political content in terms of publishing transparent information on entities paying for an online political campaign, and the amount of finances spent during a campaign. In that regard French high-ranking officials stated that their passage should provide a greater transparency of information about sponsored contents on social media, not only in terms of disclosing the identity of an advertiser, but also with regard to limiting the level of monetary amounts that could be spent on such messages. Further to this, French experts stated that the laws were passed with the view to preventing fake news from spreading disinformation during every electoral period.

Nonetheless, some of the experts hold a view that France already has an effective repressive law in this area in the form of the Republic Act of 29 July 1881 on the freedom of the press that prohibits publication or broadcasting disinforma-

tion. Thus, on the basis of its Article 27, dissemination of false news “by whatever means”, will be subject to a fine of 45,000 euros. However, the above act applies only to information that has a disturbing effect on the public peace, which is very hard to define and prove. There is also another law, being a part of the French Electoral Code, that stipulates that anyone who uses false information or other “fraudulent manoeuvres” to steal votes shall be pronounced a one-year prison sentence and imposed a monetary penalty of 15,000 euros. However, that stipulation applies primarily to cases of electoral fraud. For that reason, French political representatives are planning to ensure the implementation of the passed laws in an electoral process.

The laws foresee the introduction of a summary procedure under which judges can order deletion of a content, removal of websites from the search engines or their complete blocking. For the time being promises are made that the above legal framework will apply only to the period before an election, which is a sensitive time for every country from the political and security aspect.

EUROPEAN DOCUMENTS IN THE AREA OF COUNTERACTING DISINFORMATION

At the end of 2016, the European Parliament passed a resolution on *EU strategic communication to counteract propaganda against it by third parties*.¹² The resolution states that “the hostile propaganda” poses the main security challenge Member States are confronted with. It further notes that the hostile propaganda against the EU and its Member States is aimed at distorting truth, provoking doubts and dividing the EU and its North American partners, paralysing the decision-making process, discrediting the EU institutions and inciting fears and uncertainty among the EU citizens. Its authors conclude that effective injection of hostile propaganda into the EU’s information sphere is caused by the substantial non-supervised permeability of social networks and media that uncritically broadcast also entirely false or falsified information by continually copying news generated by foreign government-sponsored institutions and services that operate very professionally.

In mid-2018 the issue of counteracting fake news was given a significant topicality in the EU against the backdrop of launching the preparatory process for the 2019 European Parliament election. In this connection, the European Commission’s representatives demanded that media outlets and social networks immediately solve the issue of disseminating fake news on their portals, and deal with the matter of using citizens’ personal data for forecasting election outcomes in the manner of the recently published *Cambridge Analytica* case. Reacting to that initiative, Julian King, the EU’s security commissioner stated that the short-term specific plans to regulate dissemination of news on social networks were foreseen to be implemented before

12 European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)), http://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_HR.pdf

the European election when voters in 28 EU's Member States would head to the polls to elect Members of the European Parliament.

According to the statements made by representatives of the above EU's security commissioner, social media outlets are under obligation to sign a Code of Practice on Disinformation on a voluntary basis, so as to prevent the misuse of platforms for disseminating false information.¹³ The code foresees a greater transparency to enable social networks users to understand why their Facebook or Twitter accounts are targeted by a specific advertisement or content. It also put forwards that political advertising should include actual sponsor identity and amounts spent. In the event media outlets and social network platforms fail to reach an agreement, and do not commit to the above Code of their own accord, the European Commission may propose further actions of regulatory nature to make social media outlets implement the foregoing measures.

2016 saw the adoption of the *Joint Communication to the European Parliament and the Council: Common Framework on countering hybrid threats* on the EU level, which was followed by the 2018 *Joint Communication: to the European Parliament and the Council: Increasing resilience and bolstering capabilities to address hybrid threats*.¹⁴

The European Commission presented a European approach to fight disinformation online in its Communication of April 2018, pressing for a more transparent, trustworthy and accountable online ecosystem,¹⁵ and outlining actions for counteracting online disinformation, including:

- a self-regulatory EU-wide Code of Practice on counteracting disinformation signed by the major internet platforms and advertising industry,
- supporting an independent European network of fact-checkers,
- underlining the importance of secure and resilient election processes,
- fostering education and media literacy, and
- support for quality journalism.

The European Commission called to all relevant actors to strengthen strategic communication. Furthermore, in order to secure free and fair European election, it put forward on 12 September 2018 a set of measures, such as recommending greater transparency in online political advertising and targeting, and also a legislative amendment to tighten the rules on European political party funding to make it possible to impose financial sanctions for breaching data protection rules in order to deliberately influence the outcome of the European election.

13 Code of Practice on Disinformation, <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>

14 Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions, Brussels, 26.4.2018 COM(2018) 236 final, Tackling online disinformation: a European Approach, <https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en>.

15 Tackling online disinformation: a European Approach, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>

Following up on the foregoing efforts, on the European Commission presented at the end of 2018 an Action Plan against Disinformation setting out additional steps against disinformation¹⁶. It outlines the measures for a concerted and coordinated EU approach to countering disinformation in the four areas considered to be of key importance to the effective development of the EU capabilities and strengthening of cooperation between Member States and the EU, namely:

- *Improving the capabilities of Union institutions to detect, analyse and expose disinformation.* In this regard, the Strategic Communication Task Forces and the EU Hybrid Fusion Cell within the European Service for External Action (EEAS), as well as the Union Delegations in the neighbouring countries have to be reinforced by a number of additional specialised staff and data mining tools. The EEAS's budget for strategic communication, which includes implementation of activities on counteracting disinformation and raising awareness about its harmful effects, is to be more than doubled, and is expected to rise from 1.9 million euros in 2018 to 5 million euros in 2019. Member States should complement such actions by bolstering national capabilities and increasing their own resources for counteracting disinformation.

- *Strengthening coordinated and joint responses to disinformation on the part of EU institutions and Member States.* To that end, a dedicated Rapid Alert System will be established between the EU institutions and Member States by March 2019 to facilitate the exchange of information and analyses of disinformation campaigns, as well as to enable timely provision of disinformation alerts.

- *Mobilising private sector to tackle disinformation.* For that purpose, online platforms and advertising industry, as signatories to the Code of Practice on Disinformation are expected to implement their commitments quickly and effectively, while giving priority to activities connected to the 2019 European Parliament election. Such commitments specifically include ensuring transparency of political advertising, stepping up efforts to close down fake accounts active on online platform services, identifying automated bots, and cooperation with fact-checkers and academic researches in order to detect disinformation campaigns and ensure a greater visibility and dissimulation of checked contents. The European Commission will ensure a detailed and continuous monitoring of the implementation of the foregoing commitments with the support of the European Regulators Group for Audio-visual Services.

- *Raising awareness and improving societal resilience.* In addition to targeted awareness raising campaigns, EU institutions and Member States are expected to improve citizens' media literacy through specifically designed programmes. National multidisciplinary teams composed of independent fact-checkers and researchers will be set up and provided support to identify and expose disinformation campaigns on social networks.

¹⁶ Action Plan against Disinformation, <https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation>

The Action Plan against Disinformation foresees that Member States should improve coordination in tackling disinformation in cooperation with the EU institutions and other Member States in order to detect, analyse and expose disinformation campaigns, and raise awareness about the negative effects of disinformation. To that end, it also proposes activities to be undertaken by Members States, such as:

- to designate their own national contact points to participate in the work of the EU Rapid Alert System owing to which all its participating members will be provided real-time information on a situation to enable their coordinated response;
- to raise awareness on the negative effect of disinformation and support the work of independent media, fact-checkers and investigative journalists, and
- to set up multidisciplinary teams with specific expertise in a local information ecosystem.

EU'S INSTITUTIONAL FRAMEWORK FOR COUNTERACTING DISINFORMATION AND FAKE NEWS

On the institutional level, the *Task Force East Stratcom* was set up in 2015 within the European Service for External Action. So far the team made up of 16 staff members, recruited from the EU institutions or seconded by EU Member States, has documented, analysed and published over 4,500 examples of disinformation and has thus contributed to understanding tools, tactics, techniques and intentions of disinformation disseminated by foreign sources. It is planned to recruit additional 50 to 55 staff members in the course of next two years to step up the team's activities.

The core activities performed by the *East Stratcom Task Force* in cooperation with the relevant European Commission's services are as follows:

- efficient communication and promotion of the EU policies towards the Eastern Neighbourhood,
- strengthening the overall media environment in the Eastern Neighbourhood, and
- provision of support to media freedom and strengthening of independent media, as well as improvement of the EU capacities to forecast, address and respond to disinformation activities by external actors.

In addition to the East StratCom Task Force, the South and Western Balkans StartCom Task Force operating on the similar principle has also been established within the European External Action Service.

Further to this, in 2016 the *EU Hybrid Fusion Cell* was set up within the EU Intelligence and Situation Centre to monitor and counteract hybrid threats related to foreign actors, including disinformation and manipulation of political decisions in the EU and its neighbourhood.

Together with the *European Centre of Excellence for Countering Hybrid Threats*, which was recently set up in Helsinki, the foregoing bodies constitute core institutions for a reinforced EU response, and are a relevant element of cooperation between the EU and NATO in strengthening coordination and preparedness for hybrid threats.

Taking also into consideration that information sharing is a key factor in countering disinformation, the *Rapid Alert System (RAS)* was established on 18 March 2019 to tackle disinformation on the EU level. This early warning system is based on a secure digital platform enabling Member States to share real-time information on the existing foreign disinformation campaigns, and coordinate their response. The Rapid Alert System operates with open and unclassified information only, while focusing solely on foreign actors' coordinated attempts to manipulate free speech and open debates. In order to establish the foregoing system by March 2019, each Member State should designate its contact point, ideally within its strategic communication unit.

In addition to the foregoing structures, in January 2018 the European Commission set up a *High-level Expert Group on Fake News - HLEG-FK*. It is made up of 39 members (journalists, representatives of the civil society and fact-checking organisations) and tasked with advising the EU on initiatives for countering fake news and disinformation spread across traditional and social media. The High-level Expert Group on Fake News has also a sub-group that represents media, civil society, academic community and GAFA platform (composed of the Google, Apple, Facebook and Amazon representatives).¹⁷

Furthermore, an independent *European Network of Fact-checkers* is being established to counteract online disinformation across the EU. They have a crucial role in tackling disinformation because they check out and assess the truthfulness of contents on the basis of facts and evidence, thus helping towards a cleaner and stronger information ecosystem. The European Commission intends to support cooperation between the European fact-checkers to which end it will provide the right conditions for the establishment of their network. The fact-checking community will determine the pre-requisites for membership in the coming months. The European Network of Fact-checkers will be independent in editorial terms. An initial funding of 2.5 million euros is envisaged under the Connected Europe Facility Instrument (CEF) for the purpose of creating an online platform to connect fact-checkers and researchers. In the initial phase the European Commission will offer fact-checkers online tools to enable their cooperation. In the next phase it will create a secure European online platform on disinformation, which will make it possible for cross-border data collection, analysis tools and access to data on the EU level in support of cooperation between the fact-checking community and academics working on the problem of online disinformation.

¹⁷ Call for applications for the selection of members of the High Level group on Fake News, <https://ec.europa.eu/digital-single-market/en/news/call-applications-selection-members-high-level-group-fake-news>

The activities undertaken by individual EU Member States in the area of countering disinformation are illustrated in this paper by the Spanish and Bulgarian examples. Each country has set up its unit and contact points for countering fake news with a view to protecting its election processes. Thus, in view of the four elections coming up in April and May, the Spanish Government set up a cyber security group at the beginning of 2019. The group of experts will monitor hybrid threats ahead of the local, regional and European election on May 26 and a general election on April 28, while focusing on the identification on threats. As regards cyber security, all computer systems to be used in the election process will have to be certified by the National Encryption Centre to prevent an external impact. The Spanish experts point out that disinformation threats are much more complex because for the time being there are no computer tools that can guarantee the detection of fake news. Spain will task more than 100 police officers with searching the internet for fake websites and news, given that the major companies, such as Google, Facebook and Twitter are still making a slow progress towards creating programmes for detecting and labelling fake news.¹⁸

At the beginning of 2018, the Bulgarian Government also established an Anti-disinformation unit, which is positioned within the Council of Ministers and operates under the the Deputy Prime Minister's responsibility. Its establishment is enshrined in the Joint Action Plan of the European Commission and the European Parliament adopted in December 2018.¹⁹ The Bulgarian unit will be a "contact point" with the Rapid Response System to be led by the High Representative of the European Union for Foreign Affairs and Security Policy. The goals of the Rapid Response System are to ensure coordination between Member States, the European External Action Service and the real-time information exchange on false information. It is planned that the system be linked to the existing Emergency Response Coordination System, as well as to the Situation Centre of the European External Action Service (these systems operate on a 24/7 basis). The EU plan envisages that the system will work together with the existing networks of the European Parliament, NATO and the G7.

Some EU countries have set up strategic units within their Ministries of Foreign Affairs. The Bulgarian contact point - Deputy Prime Minister will coordinate activities of all relevant national authorities in connection with signals received by the system. The European system will be based on on a secure platform, enabling Member States to exchange information about foreign campaigns and attempts to disseminate fake news.

18 Spain launches unit to fight disinformation ahead of elections, https://elpais.com/elpais/2019/03/11/inenglish/1552290997_611483.html?id_externo_rsoc=TW_CC&fbclid=IwAR0XrUt9xP9IRsSyJMeEjtGGrNMHon6I3aSTfv3NAYeVP3HJMk_3ej5GXk&utm_source=newsletter&utm_medium=email&utm_campaign=kremlin_watch_briefing_european_parliament_calls_out_russia_and_calls_for_magnitsky_act_like_sanctions&utm_term=2019-03-28

19 The Bulgarian Government is Setting up an Anti-disinformation Unit <https://www.novinite.com/articles/195338/The+Bulgarian+Government+is+Setting+up+an+Anti-disinformation+Unit>

CONCLUSION

On the global and national level “traditional and new media” play a very significant role in creating public opinion, political, social and public life and, by the same token, security of national information sphere. The entry of the major media companies into media space of other countries has diminished a control of small countries over that part of national information sphere.

In the time of “information warfare” and “hybrid threats”, the legal framework in the countries that implement such operations has become a relevant factor in creating a favourable or unfavourable environment for potentially hostile actors’ activities in the information space of adversarial countries. It means that laws have a new, but very complex role in defining, classifying, and also sanctioning those threats. In this regard, a lot of EU Member States are considering ways to counteract propaganda and fake news, assessing a legislative form of such counteraction as the most efficient one.

A legal analysis of “hybrid threats” involves open issues and uncertainties due to the lack of agreed definitions of terms, such as “disinformation” or “fake news”. In this connection, criminal laws of many countries do not mention those terms. In addition, there are no specific regulations nor any judicial practice to provide explanations of regulations, and sanctioning of activities regarded as hybrid threats. Similarly, there is no sufficient state-related practice to outline how a state should respond to challenges arising from the understanding of the term “hybrid threats.” However, it is more urgent than ever to ensure that the area of national legislation should diminish possibilities of an “external factor”, in the shape of malicious individuals and groups, to exploit a vacuum in our legal environment with a view to influencing the internal political stability and security of the Republic of Serbia, particularly taking into account that in our recent history media figured as one of the most relevant factors in influencing internal developments in the Republic of Serbia, and political changes that took place in the past.

REFERENCES

1. Action Plan against Disinformation, <https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation>
2. Arquilla, J. & Ronfeldt, D. F., (1997) “Cyberware is coming!”, in *Athena’s Camp: Preparing for Conflict in the Information Age*, Santa Monica <http://www.rand.org>
3. Call for applications for the selection of members of the High Level group on Fake News, <https://ec.europa.eu/digital-single-market/en/news/call-applications-selection-members-high-level-group-fake-news>
4. Centre Against Terrorism and Hybrid Threats, <https://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx>

5. Code of Practice on Disinformation, <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>
6. Definice dezinformací a propagandy, <https://www.mvcr.cz/cthh/clanek/definice-dezinformaci-a-propagandy.aspx>
7. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)), http://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_HR.pdf
8. Final results of the Eurobarometer on fake news and online disinformation, <https://ec.europa.eu/digital-single-market/en/news/final-results-eurobarometer-fake-news-and-online-disinformation>
9. Hoffman, F. (2007), "Conflict in the 21st Century: The Rise of Hybrid Wars," (Arlington, VA: Potomac Institute for Policy Studies).
10. France passes controversial 'fake news' law , <https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law>
11. Gelfert, A. (2018), "Fake News: A Definition", *Informal Logic*, University of Windsor, Ontario.
12. Gerasimov, V. (2013), "The Value of Science in Foresight: New Challenges Require Rethinking on the Forms and Methods of Warfare," *Military Industrial Kurier*, http://vpknews.ru/sites/default/files/pdf/VPK_08_476.pdf.
13. Gerasimov, V. (2014), "The value of science in anticipation", *VPK news*, <http://www.vpk-news.ru/articles/14632>
14. Vosoughi, S., Roy, D., and Aral, S. (2018). "The spread of true and false news online". *Science*, 359(6380), 1146-1151. <http://science.sciencemag.org/content/359/6380/1146>.
15. Allcott, H., Gentzkow, M. (2016), "Social media and fake news in the 2016 election", *Journal of Economic Perspectives*, National bureau of Economic Research, Cambridge.
16. Lažne vesti i odgovor EU, . <https://europa.rs>,
17. Lohr, S. (2018). "It's True: False News Spreads Faster and Wider. And Humans Are to Blame". *The New York Times*. <https://www.nytimes.com/2018/03/08/technology/twitter-fake-newsresearch>.
18. Miljković, Milan. (2017), „Hibridno ratovannje u saveremenim domenima – primer informacionih operacija“, Tematski zbornik radova „Hibridno ratovanje – dilema koncepta savremenih sukoba“, Institut za strategijska istraživanja MO, <http://www.isi.mod.gov.rs/lat/355/tematski-zbornik-radova-hibridno-ratovanje-dilema-koncepta-savremenih-sukoba-355>
19. Miljković, Milan. (2016), „Informacione operacije u radu savremenih obavštajnih službi, disertacija, Fakultet Bezbednosti, Beograd.
20. Poland busts Russian - hybrid warfare - ring, <https://www.dw.com/en/poland-busts-russian-hybrid-warfare-ring/a-43831566>

21. Report of the independent High level Group on fake news and online disinformation, <https://ec.europa.eu/digitalsingle-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>
22. Rastorguyev, S. P. (2002) *An Introduction to the Formal Theory of Information Warfare*, Moscow. Vuzovskaya Kniga
23. Security Strategy of the Czech Republic 2015, http://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf
24. Spain launches unit to fight disinformation ahead of elections, https://elpais.com/elpais/2019/03/11/inenglish/1552290997_611483.html?id_
25. Tackling online disinformation: a European Approach, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>
26. The Bulgarian Government is Setting up an Anti-disinformation Unit, <https://www.novinite.com/articles/195338/TheBulgarianGovernment+is+Setting+up+an+Anti-disinformation+Unit>
27. Zajednički okvir za suzbijanje hibridnih prijetnji: odgovor Europske unije, Zajednička komunikacija Evropskom parlamentu i Veću od 6. aprila 2016., JOIN(2016) 18 final, <https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en>.
28. Bodrožić I, Bodrožić A. (2018), *Političko–pravni aspekti širenja lažnih vesti*, *Srpska politička misao*, broj 3, vol.
29. Stajić. Lj, Gaćinović R. (2007), *Uvod u studije bezbednosti*, Draslar partner, Beograd.
30. Parezanović M. (2013), *Politički prevrat – savremeni pristup*, *Nova srpska politička misao*, Beograd.