Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 14(63) No. 1 – 2021
https://doi.org/10.31926/but.ssl.2021.14.63.1.12

DISINFORMATION DECONSTRUCTED- COGNITION SECURITY AND DIGITAL CONTROL

Maria Magdalena POPESCU[1]

Abstract: *Fake News and Deepfakes have lately been highlighted in informative videos, research papers and literature reviews as tools for disinformation, along with filter bubble and echo chamber, polarization and mistrust. To counteract the unconventional weapons of word and imagery, a new research area has been defined as cognition security, a transdisciplinary area to understand the threats hybrid wars currently make use of and to determine the proper measures against non-kinetic offensives. For this, data mining and deep analysis are performed with digital instruments in a cognitive security system. Defined by all these, the present paper deconstructs the terms in an experimental monitoring of the media, to connect the realm of Cognition Security to its instruments in Cognitive Security*

Key words: *Fake news, deepfake, cognitive security, narrative, cognition security.*

1. Introduction

While there is an abundance of papers that delineate the context of their research by drawing on the diachronic use and meaning of disinformation and fake news, on how old the concept of disseminating disinformation is and how memorable the contexts in which fake news brought political or social instability through disseminating mistrust and polarization are, the most recent papers tackling the concept of fake news all relate the term to the pandemic times, inevitably, by bringing to attention the "block-buster" narratives- the laboratory origin of the virus, the dangers of getting vaccinated, triggering mistrust in the medical system along with the harm that the government and its institutions have been trying to inflict on us, the people, by placing society in a successful "us versus them" pattern. They all have managed best when the core of the narrative speculated old cognitive patterns or inherent fears, coupled with national tragedies or inherent beliefs. Translated into the social media realm where people gather to gain acceptance, appreciation and share emotions, all narratives escalated

[1] *Carol I National Defense University,* popescu.maria@myunap.net.

both in dissemination and in their influential power, aided by machine learning, software agents and specially trained individuals to act to this end.

What is alarming is that more often, beside artificial intelligence, the spread of such (dis)information is performed, in many cases, with socially acknowledged public persons that borrowed from the advertising mechanism and act similarly with what influencers are known to do today - people with public recognition, socially placed at nodal points, which allow them to spread ”professional” statements, similar to contingent reality trolls- among them one counts lawyers, academics, writers, film producers, doctors or vloggers, as real persona or even a deepfake representation of what is real, as a European report on disinfomation states (Eurocomunicare, 2020).

1.1. Fake News, Deepfakes, Bots, Trolls, Filter bubbles, Echo chamber

To counteract the malicious harnessing of artificial intelligence and machine learning, research has extended its tools on a mission to stop „growing public cynicism, social distrust and even technophobia, as the rise of echo chambers, fake news, disinformation and the deliberate *weaponisation* of information by state and non-state actors have fuelled fears of digital technologies having unintended consequences that may actually undermine rather than strengthen the social fabric of Western societies” (Bjola and Pamment 2019, 48-51). Understanding the terms seen as instruments for sowing mistrust and their mechanisms, researchers can corroborate information to understand, debunk and thus raise awareness, through dissemination, over the implications online behavior has in enhancing the seabed for malicious use of digital content and digital communication space. By fake news this paper covers the related terms of *post-truth* and *post-fact,* as such: ‘*fake news’* is „fabricated or false information that is disseminated through public media channels, including print, broadcast, and online” (Lazer et al., 2018, p.1094-1096) which is also referred to as *post-fact*, the information that inclines more to value opinions to the detriment of facts and as *post-truth* (Berthon and Pitt, 2018, p. 218-227), which manifests itself as the state of affairs when “objective facts are less influential in shaping public opinion than appeals to emotion and personal belief” (Oxford English Dictionary, 2018). Conversely, *deepfakes*, take us to audios or videos of real people who state facts they never said or did by neural networks”. This has been „widely used to forge politicians’ speeches and illegal evidence, resulting in hurting public feelings and affecting the political situation seriously” (Agarwal et al 2019, 38-45; Floridi, 2018, p. 317-321; Korshunov and Marcel, 2018). A large scale publication, *Science,* explains the formation, replication and influencing mechanisms that the phenomenon *fake news* depends upon. (Loo Seng Neo et al 2020, 241-263). Moreover, analyses performed by Ruths (Ruths, 2019, p. 348-348) reveal five agents that support the dissemination of fake news- publishers, authors, published materials, audience or the public readers and the rumor spreading phenomenon, all these being successful in their dissemination. These are extremely effective because the social networks and online content have overwhelmed and drowned individuals’ attention and power to concentrate, generating confusion, shallowness in approaching information, which, the more it is, the more trusted it becomes, thus entailing a feeble resilience and a more

acute tendency to lend one's trust to any shared content, without prior verification, along with a frequent disposition to co-create and share, to the benefit of information warfare warlords.

While *bots* as artificial intelligence software perform rapid repetitive tasks imitating human behavior, with various goals like scanning messages or information content, learning it and being able to provide the exact information when it is needed through the search engines (web crawler) , to attack a given target, by interacting with a page, within a social network, by imitating human users, generating follows and likes in social media(social media bot) or to automatically chat with various users in commercial websites by answering with predetermined phrases (chat bot), their partner in lexical co-occurrence, *trolls* are human users in online communities. Trolls' main purpose of interaction or online presence is to bring up hate speech, flame wars or saw discord, aiming, on a long term, to develop reluctance and insecurity in those under attack, but also to generate feuds within certain groups, on off topic subjects. For this, they will augment any negative information or they will make up new unreal ones, repeatedly posted with an aim to make it all believable. Trolls make use of language in general, they appeal to manners in which messages are constructed and to the way they are delivered- for example they take an aspect out of context so that, framed differently, the same aspect can have double meaning. Some other times they raise a detail to a general level, in order to augment the core event and share it in a different light. In a contrastive approach, bots are responsible for the dynamics of the messages while trolls are focused mainly on the content. A third-layered approach beside the two already mentioned ones are two other human-performed instruments: the selection of marginal opinions and the personal attack meant to give way under pressure and accept the idea imposed. One example can be "the state is me", which advances authoritative figures who once had stated something similar to the fake content. Both these instruments generate confusion while gaining confidence from the followers, simultaneously. All of the above mentioned instruments, artificial intelligence or human driven ones, control the content area.

In addition to the previously mentioned instruments, *filter bubbles* and *echo chambers* are created from an extreme users' personalization attitude, from an extreme "fear of missing out" (FOMO). Driven by FOMO, ideologically and culturally isolated individuals are fed with information provided by Artificial Intelligence agents which replicate the searching behavior and interest based on geo-location and previously referred content to end up separated from the views one disagrees with, actually self-isolating within one's own cultural and ideological *bubble.* Driven by their own interests, individuals, fueled by software inside a *bubble*, are driven away from the possibility to refresh ideas, to be contradicted and forced to approach knowledge at a deeper level. This fuels disinformation through isolation and through a personal interest filter. Meanwhile, the new information that contradicts the individual's interest is extremely low. An *echo chamber* replicates the same information the opinion leader or the source has disseminated, information that is replicated by those whose opinion reflects the same views. Misinformation can thus be driven by the lack of opposing views and the tendency for confirmation bias (an inner need to favor existing beliefs) By

comparison, the two terms show the difference between humans and AI: the filter bubble is algorithm-driven, while the echo chamber is human generated, opinion leader- voiced. Mistrust and polarization are generated in the process of consuming fake content in isolation, supported by confirmation bias and influencers within each echo chamber.

2. Cognition Security (CogSec) and Cognitive Security

Encompassed by all of the already mentioned aspects, supported and strengthened by EU policies and by national defense strategy, a better understanding of the phenomenon would empower social resilience and would counteract malicious narratives. To this end, a new area of research has come into effect, *Cognition Security (CogSec)* which acts on the one hand to identify the hostile acts in virtual environments and then, through the protection component, to debunk the fake news and deepfake phenomenon by unveiling communication patterns and the dissemination strategies, by understanding the cognitive behaviors underneath and the way humans, aided by software agents, interact in sharing the information. All this triggers a trans-disciplinary approach „that leverages knowledge from social science, psychology, cognition science, neuroscience, AI and computer science" (Guo et al., 2021). In this context, *cognition security* relates to terms already advanced in social media, beyond fake news and deepfake, looking at the process of information consumption and communication by large- polarization, bots and trolls, filter bubble and echo chamber, to understand and reveal their structure, to understand their mechanism and thus be able to counteract the ways in which disinformation generates an erroneous opinion formation. Drawing the line for these important terms, what they all have in common is cognition, language, psychology, sociology, and artificial intelligence, all translated into media channels, where not only news but also entertainment can become weapons of political warfare, once these serve as sources for the vulnerabilities a society can have. Studies on cognition and psychology reveal patterns for developing personal opinion different and proper to each state, based on its own cultural values and socio-political experiences, since threats to a state now come within the realm of linguistics and socio-cultural aspects that communicate their scope in embedded words and imagery specific actors resort to, in accomplishing their goals. By performing a close analysis of all these, one will estimate how vulnerabilities can be turned into strong points, with all the threats identified. *Cognition Security* as a new field of analysis is focused on the impact fake news has on human cognition with all its aspects-misperception, attitude formation, decision making- and looks at ways to counteract this impact, with the help of social science, psychology, cognition sciences, AI. This can be done with all digital technologies that perform real-time data analysis and identify cognitive hacking, seen as manipulation of human perception with misleading data that perform disinformation, as well as with machine learning used to understand the abundance of information impacting human cognition.

3. Digital Control Instruments

Knowing what people need from the online environment, which are the searching lexical habits and how fast information travels and undergoes development generates insights into how the architecture of information is manipulated and to what ends, giving thus clues on how to control and even counteract both hostile actors and their malign action. In approaching the lenses to look at the information and communication processes social media fuels in generating both malign and benign type of content, various research reveals that people resort to certain categories of information today, while they are overwhelmed by the abundance of what this consistent search overflows. Close analyses have revealed that there are four areas people are constantly interested in, throughout their online existence (PAHO, 2020)– they need information from the government (government decisions, public administration measures and data), information used for education and training (online courses, webinars, educational materials or sites disseminated in social media), information with social impact (medical interventions and updates, social and civic emergency management and control) and news about what happens in the world, at international level (interactions, management, policies and data) In a close analysis, research papers are abundant in the already mentioned category related words. Based on their scope, these words can be organized in clusters, namely- information related to media, audience reaction, communication for interpersonal messages and concepts, represented as such in the diagram below, provided by a *Defense StratCom* analysis: the words related to media are in green, those related to audience are in red, those related to communication are in blue, while those in yellow are conceptual, general.

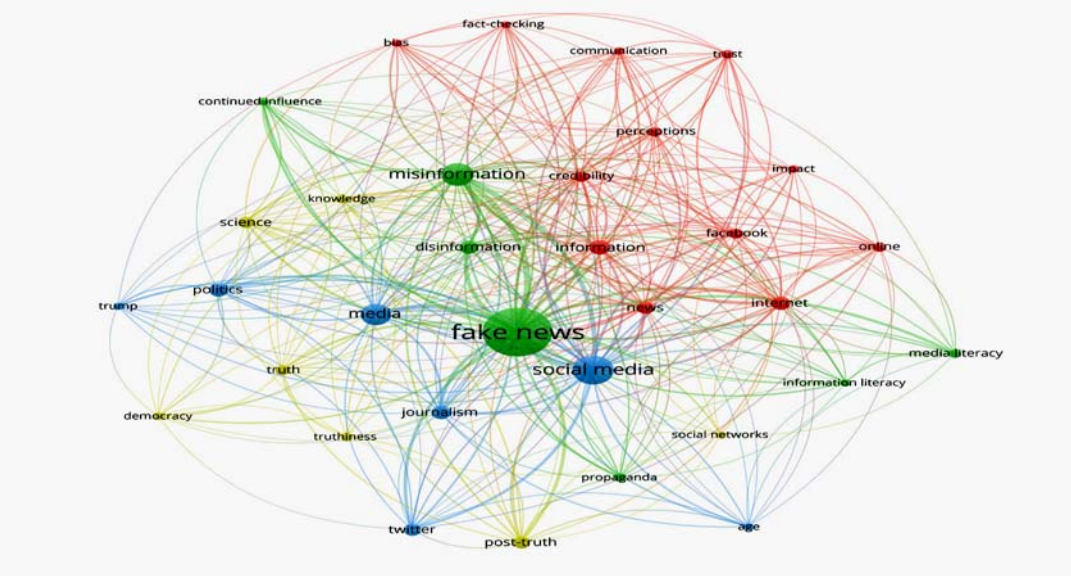

Fig. 1. *VOS viewer representation of co-occurrence analysis on fake news related terms (Defense StratCom, 2020)*

This information reveals consequential connections among the areas people expressed interest in their online searches and the lexical clusters created on the most frequent terms that appear in their searches. Thus, individuals look at everything social networks and online space provide to get their information related to government, to educate and train themselves but also to understand decisions, policies and regulations that impact society, in addition to being spatially and temporally anchored through the news from the world. Individuals consume media, communicate to exchange information, pay attention to the peers' interpretation of the surroundings and consult scientific publications for objective information, as seen in Table 1.

Types of information people need and sources to obtain it Table 1

Government information	**Media, interpersonal communication, audience reaction**
Education and training information	**Media, interpersonal communication, science**
Social impact information	**Media, interpersonal communication, audience reaction,**
News about the world	**Media, interpersonal communication, audience reaction, science**

The amplitude information gains and has gained even more in pandemic times accommodated by superficial processing and random selection, accompanied by a shallow knowledge of how cognitive skills and critical thinking are, used into a play of influence and propaganda needs an accelerated and thorough understanding of how and why disinformation has been so successful. *Cognition security* approaches the impact disinformation has on human cognition with the goal of changing attitudes and influencing the decision making process through misperception and distrustful information and knowledge, and, seen as a process, it is meant to ensure humans' safety from being affected by false content. This can be provided by revealing the cognition and detection techniques and how the bots and trolls are a danger to knowledge acquisition and opinion formation, simultaneously revealing echo chamber and filter bubble manifestations. The studies focusing on the type of information needed and the most frequent words used in the process of information search reveal the paths and pools the disinformation agents get inspiration from, in designing their messages. This reveals where they can find the places and the keywords which may lead to the targeted public. Even though considered strong points, these studies can become vulnerabilities but, at the same time, they can be a raising awareness instrument for hostile actors as well.

Cognition Security as a newly outlined research area is mainly meant to counter-act against all those state and non-state actors that use social media for malicious acts, by performing analysis and deep check on the instruments and strategies the hostile actors use in generating narratives.

Cognition security deconstructs all of these processes in a search to reveal the mechanisms and to find an effective counteraction against alternative realities

generated by conspiracy theories that fuel propaganda and weaken democracies. To accomplish this, experts ground their analyses on the largely debated *theory of reflexive control* (Jaitner and Kantola, 2016, p. 27) the Soviet concept of influencing the adversary's decision making process, to approach the content strategies analysis. The reflexivity refers to an actor's endeavor to adjust his actions based on the opponent's decisions to operate, relying heavily on command and control, cybernetics, decision making and information warfare to analyze how propaganda and disinformation campaigns run. The theory consists of two directions (Vasara, 2020) the constructive one which influences the enemy to make the decision the initiator aims at and the destructive one, which induces mistrust in the targeted actor's decision making process. Also, the instruments of reflexive control cover manipulation, disinformation, hard power, to act upon the receptor's decision making process, and to impact his answer, at the same time (Thomas 2004, p. 237-256). More than the mechanisms used to perform that, the timeframe and the traces a high impact narrative may leave, from moment zero to the finals, valid for any scenario of spreading content, are explicit in the diagram below:

Fig. 2. *The way information travels and spreads itself (Delaware County Community College)*

Figure 2 depicts the itinerary information takes when an event is shared, within minutes, from occurrence in social media, irrespective of the content (short message,

multimedia, imagery, video or online opinion text). In a few days, the information is processed and becomes a material for the newscasters, then background information is added within a week, to be used in longer periodicals (magazines), then the idea is taken over by researchers interested in the field and it becomes the basis for an expert development, a research material, within months. If this becomes utterly largely debated and is given extra interest from society, the topic may well become the topic of books. Understanding how information travels and how fast it can, by augmentation, get universal proportions is a step forward in seizing the importance of debunking the false content and thus stop it from spreading, or, if seized too late, identifying the source with reverse engineering, and stopping it from generating other products.

3. CogSec Approach to China's Online Activity

To connect all the deconstruction of terms and practically show the result of their action, this section will highlight that while analyses on Russia's disinformation abound and most of the analysts target their attention to its highly debated strategies, studies in the field have lately concentrated on what happens in Asia in this respect, especially in what China as a prominent disinformation and propaganda actor does.

Chinese communicators and strategists base their course of action on Sun Tzu's vision, with "Better attack people's mind- than fortified cites", and this is visible in the Chinese decision to use the media and the social media to attack the minds and win the hearts of Europeans. However, while China is silently unfolding an innuendo into the western world, the step is still poorly represented in current studies in the field. The present paper is thus aggregating information available through *Riga StratCom CoE* resources with information presented in the international media, trying to highlight the importance of strengthened and complex digital control analyses seen at trans-disciplinary crossroads between language, psychology, artificial intelligence and cyber security.

A generalist approach sees China's global information system in a permanent development, with a surge in aggressive messaging in pandemic and a much higher traffic on western social media platforms, especially on Twitter and Facebook, where Chinese diplomats and diplomatic embassies have migrated. Analyses have revealed that about 100 accounts have been created since September 2019, all meant to send messages to the diplomatic core, to increase China's fighting spirit and its international voice, to build itself a global media presence. This is shown by creating content and broadcasting it in multiple languages across various social media platforms, or by disseminating ideas and opinions after gaining editorial space in western European publications, from *The Washington Post* to *Helsinki Times*, indicating that China's global information machine has been active, as Erika Kinetz, Shanghai correspondent for Associated Press put it. China's global information architecture revealed how re-distributing messaging across languages and across platforms, across countries, works in pandemic times, with the infrastructure it has, even though a control over how many followers are real and how many are fake or who is actually getting the effect of the message is impossible, and this is what China speculates in its information architecture.

Moreover, the evolution of China's messaging strategy has witnessed a change from positive to negative messaging and also an increased aggressiveness. If China's propaganda focused on highlighting the virtues of the country and people before, in pandemic times China seemed to be Russia's disciple, using Russia's toolbox in disinformation, to promote misinformation, active disinformation (one of the examples narrates that the coronavirus was created in the US military lab and brought to China) and to exploit weaknesses and division. Moreover, there was a change in its propaganda too, with a shift towards negativity, raising China's profile as a big power and also spreading conspiracy theories difficult to align, all to gain followers on western social media. As Linda Curika, Communication Officer at NATO StratCom CoE stated, studies have shown that China has a different messaging system, customized for internal and external audiences separately.

The disinformation or the information offensive seen in China during the Covid-19 pandemic concentrated narratives on topics like: China has a good authoritarian system, China is good, while foreign countries are unstable and not trustworthy. China builds for itself a reliable image as promoting the social and political model of the 21st century, on a global scale, with varied success, being very careful in maintaining a politics of denial, spreading conspiracy theories on social media but actually sharing them as things posted by a third party initially, to avoid self- attribution. In some countries the narratives thus spread and went down very well, while other people were offended by the pressure imposed for praising. What is more, they have been making constant efforts in relation to the media with counter narrative about Wuhan as the origin of the virus, (they did not publish a EU diplomat's letter until the reference to Covid-19 initiated in China was removed) and they targeted all these acts for the European audience.

To exemplify with data, an experimental and randomly selected international media monitoring aggregated information on China's strategy which mainly spins around the COVID-19 pandemic and the relations to other states:

- the EU foreign affair J Borell stated they don't have the manpower to counter the hybrid attacks coming from China.
- most of the narratives part of the massive disinformation campaign spinning around the COVID-19 pandemic were generated on topics about a virus seen as a bioweapon produced in the US.
- China, Russia and Iran played the reflexive theory game in manipulating information and strengthening its core with multiple re-iterations across Europe
- China spreads disinformation about the non-Chinese vaccines, mainly feelings of doubt about the western produced vaccines. As reinforcement, the cases of people who died in Germany after the vaccine have been spread in a material by a media anchor.
- Based on AP reports and Atlantic Council, China was backed up by the US, Iran and Russia in the massive virus disinformation, with China issuing counter narratives to the US content, aspects which specialist state as not true.
- China advanced narratives in a post-World Health Organisation control of Wuhan lab, inferring that the US should be placed under scrutiny as well. Moreover, other theories mention the governmental failure as well as theories that imitate those

blaming the lab procedures in Wuhan, which leaked the virus from a pathogen related experiment.

- Apart from disinformation tools, China has been using heavy duty non-conventional, hybrid artillery- to criticize the US and defend China in the pandemic narratives based on virus origin, discrediting the vaccines used and distributed in the US, through fake Youtube, Facebook and Twitter accounts, actions backed up by public figures acting as influencers to spread propaganda in contexts like Latin America, Pakistan and Hong Kong.
- Chinese disinformation apparatus appeals to mock experts that use academic language and bring arguments from scientific research to gain credibility and insert the idea that the Australian Chinese people will turn into genetically modified humans if they take the vaccines from Pfizer. Asked to confirm or deny, China has always declined any involvement in these messages.
- As a reflection of all of the above, the Romanian social media was a dissemination ground for these narratives as well- resulted in the reflexive theory game played by China and Russia and Iran, as Associated Press and NATO reports have concluded- the conspiracy theories about vaccines, the danger of producing genetically modified humans, the amplitude of the Norway vaccinated victims, the incapacity of officials to manage the health crisis, which all culminated in a lowered confidence in the state institutions, especially in the Ministry of Health and its staff. Moreover, the confusion created and the mistrust that sow division between the state and society is deepened through a schism at educational level (regarding decisions on how to organize a continuation of the educational process under all these imminent dangers)

4. Conclusions

In the long debated and researched contexts that appeal to disinformation and asymmetric warfare, the high frequency weapons such as word and imagery along with software agents and machine learning have triggered a new realm to come to dawn- Cognition Security or CogSec. Cognition Security has been called upon as a means to detect and understand the hostile acts and plan a response strategy against those that act to bring confusion and weaken trust between state institutions and society. In order to be performed and to generate analyses followed by protection or counter action, Cognition Security relies heavily on Cognitive Security instruments and it needs to correlate its actions with digital control in order to gain intelligence and understand patterns of action in communication, interaction, posting and messaging. Examples of these reside in the reflexive control theory or in the word clustering classification presented in this paper. To understand the manner of expressing the messages in a narrative, to see where an actor distributes and disseminates its messages and which is the strategy it applies for this, which are the great powers that relate to this manifestation and how the digitally learned behaviors support and feed all this means to understand how all these become threats to humans but also to allow for identification of a counter act in order to either annihilate or strengthen resistance in

front of those who plant reluctance and eventually- mistrust. Used in correlation to a media random monitoring, these instruments show how cognitive maps can be created with the information gathered in a better understanding of the malicious actor. In connection to the information gathered through the media monitoring exercise, concise profiling can be created (the example in this paper is about China) - the initiator produces a disinformation strategy based on the opponent one, here- China's mingle with the US and Russia at the same time. China borrows ideas from Russia to attack both the US and Europe. It enters Europe aggressively, with a plan to ask for praise that is too intrusive and it changes the content and message building tactics. A counter active strategy will try to defeat the enemy's malicious intent. The paper highlights and confirms that a better understanding of the key words and of the way they are spread can generate patterns of interaction and predict hostile acts in the asymmetric warfare based on word and image. For this, a cohort of language specialists is needed, along with data engineers that would tackle predictive analytics and all generate models to then fill them in with tailored counter-weapons.

References

Berthon, P., Leyland, P. (2018). Brands, Truthiness and Post-Fact: Managing Brands in a Post-Rational World. *Journal of Macromarketing*; *3*8(2), 218-227, https://doi.org/10.1177/0276146718755869

Bjola, C., Pamment, J. (2019). *The dark side of digital diplomacy*. London. UK, Routledge.

Bolt, N., Karen, A.L.A., Siman-Tov, A., Fridman, O., Javier, I., Colley, C.T., Granelli, F., Althuis, J., Mitsu, C.F. , Plangger, K., Pitt, L., Snow, N., Park, A., Montecchi, M., (2020). *Defence Strategic Communications* Vol. 8, Autumn, DOI 10.30966/2018.RIGA.8.4.

Delaware County Community College: *Fake News: Evaluating Current Events Coverage,* retrieved from https://learningcommons.dccc.edu/c.php?g=609709&p=4232862

Department of Evidence and Intelligence for Action in Health- *Understanding the Infodemic and Misinformation in the fight against COVID-19*, retrieved from www.paho.org

Eurocomunicare-*(*2020)-*Raport-infodemia-COVID-19-in-România-[COVID-19 Infodemia report]*retrieved from https://www.antifake.ro/wp content/uploads/2020/11/ Eurocomunicare_Raport-Infodemia-COVID-19-in-Romania_octombrie-2020-1.pdf

Floridi, L. (2018). Artificial Intelligence, Deepfakes and a Future of Ectypes. *Philosophy and Technology.* **31,** 317–321 https://doi.org/10.1007/s13347-018-0325-3

Guo, B., Ding, Y., Yueheng, S., Ma, S. & Li, K. (2019). The mass, fake news, and cognition security. *Frontiers of Computer Science* 15 (3), DOI:10.1007/s11704-020-9256-0

Jaitner, M. & Kantola, H. (2016). Applying Principles of Reflexive Control in Information and Cyber Operations*, Journal of Information Warfare,* Volume 15, Issue 4. Lurray, USA retrieved from https://www.jinfowar.com/journal/volume-15-issue-4/applying-principles-reflexive-control-information-cyber-operations

Korshunov, P., Marcel, S. (2018). *Deepfakes: a new threat to face recognition? assessment and detection*. retrieved from https://arxiv.org/abs/1812.08685

Lazer, D., Baum, M, Benkler, Y., Berinsky, A. (2018). The Science of Fake News; in McManus and Michaud. *Never Mind the Buzzwords',* Science. Vol. 359, issue 6380, 1094-1096, DOI: 10.1126/science.aao2998

Oxford English Dictionary (2018). www.oed.com

Ruths, D. (2019). The misinformation machine. *Science,* vol.363, no.6425, pp.348-348, https://science.sciencemag.org/content/363/6425/348.summary

Shruti, A., Hany, F., Yuming, G., Mingming, H., Koki, N., Hao, L. (2019). Protecting World Leaders Against Deep Fakes. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops.* IEEE, pp.38-45. Long Beach, CA, USA.

Thomas, T. (2004). Russia's reflexive control theory and the military. *Journal of Slavic Military Studies*, 17:2, 237-256, DOI: 10.1080/13518040490450529

Vasara, A (2020). *Theory of Reflexive Control Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy*. National Defense University, Helsinki, Finland.

Xingyu, K. C., Heng Hong, T. (2020). Identifying Factors That Propagate The Spread Of Fake News, in Loo Seng Neo, *Prepared for Evolving Threats.* 241-263,World Scientific Publishing, Danvers, MA, USA, retrieved from https://www.worldscientific.com/worldscibooks/10.1142/11812#t=suppl