EMC Submission No 79
Received 29 September 2020

Observations on

Misinformation, Disinformation, and Malinformation

in Digital Media

Submission

to the

Electoral Matters Committee of the Parliament of Victoria

29th September, 2020

Dr Carlo Kopp

The deluge of misinformation, disinformation and malformation that pervades digital media[1] of all type has been justifiably labelled a pandemic[2]. Australia, like other democracies, has not been immune: this deluge of falsehoods has produced social discord and adversely influenced public understanding of a wide range of policy matters, most recently the SARS-CoV-2 / COVID-19 pandemic. Foreign nation states and non-state actors have both been major producers of these falsehoods and therefore merit close attention – both have arguably produced impacts on major votes overseas and we should expect to see spillover effects in Australian federal and state politics due to the globalised distribution of content in digital media.

The author has been conducting research in Information Warfare since the early 1990s, and since 1999 has explored how to mathematically model deceptions such as "fake news" and their impacts on large and complex social systems.

Jointly with Drs Korb and Mills the author published research in late 2018 that exposed both the sensitivity of a population to the effects of *"fake news",* and the sensitivity of *"fake news"* to costs incurred, leading us to subsequently provide evidence to the UK Parliament's DCMS Select Committee's *Inquiry on Disinformation and 'Fake News'*, and the JSCEM in Australia. Many observations in this submission are drawn from that evidence.

Biological versus Digital Pandemics

The best starting point for appreciating the potential and actual impacts of the deception pandemic in digital media is to explore the remarkable similarities between the spread of deceptive content in digital media, and biological pandemics.

An important finding from our 2017-2018 research effort was that deceptive messaging in social media can produce serious disruption in consensus forming behaviors in groups of users. Since democracies rely upon some degree of consensus to function, these disruptive effects can produce impacts out of all proportion to the effort invested in producing them.

We found that even a remarkably small percentage of deceivers in a population, in our simulations less that 1%, could catastrophically disrupt cooperative behaviours in the simulated population.

[1] We define "digital media" as the whole system of digital content creation, distribution and storage via social media, electronic mail, encrypted digital messenging tools, and websites, accessible to the public.

[2] We employ the EU definitions, where misinformation is *unintentional*, disinformation is *intentional*, and malinformation is the *exclusion of critical facts* to produce a misleading conclusion or false belief in the mind of the victim. The latter is a common feature of narrative driven hyper-partisan media coverage where facts are considered less important than partisan narrative.

In the extreme case of cost-free deceptions, where *"fake news"* producers in the simulated population are unhindered in any way, cooperative behaviours vanished altogether. Put bluntly, almost everybody ended up deceiving everybody else, as competition to survive individually displaced any effort to cooperate to survive.

A related and very important observation, not widely understood, is that the traditional view of propaganda as being intended to "turn" an audience to the propagandist's viewpoint is incomplete.

In general deceptions can produce two possible impacts on a victim.

The first of these impacts is a false belief, that represents the traditional intent of propaganda, and the other impact is uncertainty or confusion, that tends to cause decision paralysis in its victims.

Contemporary propaganda deceptions often aim for no more than to create uncertainty or confusion in victim audiences, that might otherwise require significantly greater effort to "turn" to the propagandist's asserted viewpoint. Confused consumers of such information will often withdraw from a debate leaving the field to the propagandist uncontested. There are indeed documented instances of this approach being employed to discourage US voters from participating in an election.

The focus on creating uncertainty and confusion in a population is a well documented feature of contemporary nation state propaganda, a model pioneered by Russia over the last fifteen years following the catastrophic Cold War era failure of the established Nazi and Soviet model of "turning" audiences to the propagandist's viewpoint.

Another related observation is that empirical study of social media data and agent-based modeling and simulation of deceptions in social media show that the spread of social media deceptions often exactly fits widely used mathematical models originally developed for modelling the spread of biological pathogens.

The main and critically important difference in the spreading of social media deceptions is the timescale and footprint, as a person infected with a biological pathogen might on average infect another five people, and this might take several days to happen. When deceptions are spread in social media, the "digital pathogen" can be spread to millions of people across a social media platform in almost as little time as it takes to read the message and hit the "share" button.

Much of the success of digitally distributed propaganda and deceptions conducted by nation states against Western democracies is a direct consequence of the inability of Western governments to respond quickly and effectively to such attacks. Traditional media communications and public relations techniques are simply too slow to keep up, and victims are influenced before they can be defended from the attack. By the time the government agency has responded, the deceptive idea has been accepted as uncontested fact and the victim has been led astray.

The similarities between biological and digital pandemics extend well beyond analogous spreading behaviours.

A critical problem observed in the COVID-19 / SARS-CoV-2 pandemic, but also a feature of the recent public revolt in Belarus, is what epidemiologists term *"cryptic transmission"*, where the pathogen is being quietly spread by asymptomatic or pre-symptomatic patients. As no cases end up being detected, they cannot be identified and isolated to protect others.

We observe a directly analogous problem with email and encrypted messenger tools such as *WhatsApp*, *WickrMe* and *Telegram*, which have become covert channels for the distribution of messages (notable case studies being a deceptive claim in Nigeria spread via *WhatsApp* about the use of hydroxychloroquine that led to multiple cases of overdose and hospitalization, and the use of *Telegram* by the Belarusian pro-democracy protest movement to organize and synchronise protests – "cryptic transmission" can be used for bad but also good purposes).

The popularity of such encrypted messenger tools is because they frustrate intrusive surveillance by governments and platform providers – this equally so frustrates provider efforts to locate and delete deceptive and especially dangerous messages.

For years the author has repeatedly received multiple requests from friends and colleagues concerning such messages being spread by email – "*is this a fake or not?"* – and in most instances the messages were indeed fakes. Often these fake reports were artfully crafted so that only a subject matter expert would recognize that they were actually fakes.

Another notable similarity between biological and digital pandemics is that both biological and digital pathogens mutate and evolve over time, as they adapt to their victims to maximize their spread. In social and mass media, these mutations clearly arise as a narrative or claim is misunderstood, or embellished while being spread. The rapidly evolution of false and misleading narratives and claims presents serious challenges in public communication and education, presenting the proverbial *"moving target"* for governments trying to deal with widely accepted falsehoods being spread. It can also frustrate automated tools searching for falsehoods where these depend on prior knowledge of the falsehood.

Where there is uncertainty, anxiety, and a lack of understanding, false and misleading narratives and claims find fertile ground.

The currently and ongoing COVID-19 / SARS-CoV-2 "deception pandemic" is a valuable case study as it has seen strategies previously deployed in a disparate manner to cause mayhem during elections, employed more widely and more systematically.

Propagation of false and misleading claims during the COVID-19 / SARS-CoV-2 "deception pandemic" has been via multiple channels including:

1. Social media platforms where nation states, non-state actors, media and public introduce or propagate falsehoods;
2. Private communication channels such as encrypted messenger tools and electronic mail, where nation states, non-state actors, and public can introduce or propagate falsehoods;
3. Mass media platforms and channels, where nation states, non-state actors, and public are given opportunities to introduce or propagate falsehoods;

A major concern during this pandemic has been the role of careless or agenda-driven media organisations in spreading false and misleading narratives and claims. A recent study by Tsfati et al shows this is a pervasive problem and a major contributor to the spread of social media falsehoods.

This is also an instance of the *"proxy delivery"* problem.

The problem of *"proxy delivery"* has been well studied and was analysed in detail over a decade ago by this author. That research determined that "*proxy delivery"* was a major *"force multiplier"* in the distribution of toxic propaganda – the specific case study was that mass media distributing violent media content produced by terrorists were directly acting as proxies for the terrorists producing the propaganda, whether they knew it or not. This problem was also directly identified in the UK DCMS *Disinformation and "fake news" inquiry*, and elsewhere.

While public trust of media organisations is now lower than a generation ago, the public will often see media propagation of a claim or narrative as validation or legitimation of the narrative or claim, increasing potential acceptance of a falsehood as fact. Therefore media are a valuable *"proxy delivery"* channel for foreign propagandists intent on disrupting Western democracies, and frequently targeted with content that might be seen to be attractive.

In the Australian context an excellent case study is the deception campaign launched by Russia in 2014 to divert blame for the destruction of MH17 by Russian Army 53rd Air Defence Brigade missileers deployed covertly in Eastern Ukraine and the resulting loss of almost 300 lives. At the time many Australian media organisations rebroadcast Russian supplied B-roll and footage including deceptive narratives. Judging from recent survey data (Pew) and at least one recent publication, many of these well documented falsehoods remain uncritically accepted as fact in parts of the Australian community.

Careless spreading in mass media appears to arise most often when journalists or media organisations make no effort to validate or verify content before they propagate it, or simply lack the understanding of the subject matter required to find out how to validate it, or that it should even be validated. This is a common problem but is often expensive to correct as experts with understanding of an area are much more expensive to hire than lay media personnel. Even if an expert is happy to comment *pro bono*, time and effort is usually required to find and engage one.

Much more problematic is the intentional "fitting" of content to existing narratives by hyper-partisan players in the mass media. This can range from excluding facts to embellishment of reports to support a specific agenda, such as promoting or diminishing a politician or political party – most of which constitute deceptions and fit the malinformation definition. While such behavior is highly disruptive in a political debate, it can have lethal consequences where it creates false beliefs or uncertainty – a good case study are safe behaviours during a pandemic, or the benefits and risks of using specific medications or treatments.

There are indeed numerous good case studies to be found in the SARS-CoV-2/COVID-19 pandemic. An instance is the ongoing controversy over chloroquine and hydroxychloroquine, where media organisations have either promoted or diminished the efficacy of this medication, depending on their political alignment, while actual medical trials and studies were and are still under way and the final outcome is yet to be determined. That a number of governments and other organisations have responded to media coverage by suspending or halting trials before the trials have been completed and evaluation of the results is complete shows how destructive this kind of media partisanship can be, and no credit goes to those governments and organisations who put media approval ahead of the potential to deal with the disease. Knowing with certainty that a medication does or does not work, or under which conditions it does or does not work, is valuable knowledge that can save lives. Impairing the acquisition of such knowledge to promote partisan political or commercial agendas is simply not in the public interest.

Another feature of the COVID-19 / SARS-CoV-2 *"deception pandemic"* is the extensive use of proxy groups, comprising both activists and supporters, to promote and propagate deceptive narratives and claims in both social and mass media.

The employment of agenda driven domestic entities to cause mayhem and disruption with direct social and political impacts is not a new phenomenon and arguably is an extension of the subversion techniques developed by the Soviets during the interwar period to force regime change. Indeed, most of the foreign influence practices conducted in digital media by adversaries of Western democracies are no more than a "digital refresh" of classic Komintern and Soviet propaganda, disinformation, and subversion techniques, widely employed during the Cold War using print media and broadcast radio.

The Russian government has been repeatedly implicated in promoting anti-vaccination groups in the US to simply produce social disruption and reduce public confidence in the medical system and government. Broniatowski et al two years ago detailed an extensive Russian campaign using Twitter bots and trolls to amplify the extant anti-vaccination debate in the US.

The appearance of the `#DanLiedPeopleDied` *Twitter* hashtag in August this year is another useful example, as it illustrates multiple effects. The hashtag was initially distributed via an inauthentic Twitter account, and further propagated by other inauthentic accounts to start a debate over the veracity of the Victorian Premier's statements on the pandemic. Graham observed that *"Even if getting #DanLiedPeopleDied to trend was not the result of a disinformation campaign, the outcome serves the goals of disinformation: to drive a wedge into pre-existing fractures in society, to confuse citizens and cultivate distrust in democratic institutions and authorities."* This attack illustrates the globalised nature of the problem as the inauthentic accounts in question were previously used for attacks in countries other than Australia (the ownership of the accounts is yet to be disclosed), and the attack was clearly aimed at producing uncertainty and disrupting community consensus mechanisms.

More recently we have seen an alliance of convenience formed between some anti-vaccination groups and the 5G conspiracy theorists, the latter who assert that contrary to radio physics and virology 5G cellphone emissions are the cause of the pandemic, rather than the SARS-CoV-2 viral pathogen. Russia has actively promoted this agenda, and employed mass media such as RT to propagate quite absurd claims that these radio emissions are dangerous even prior to the pandemic. More recently Russia has been implicated in the support of 5G activists in Europe, some of whom have even conducted arson attacks against 5G network installations. The result of such sabotage can be the loss of mobile communications, impairing access to medical care during the pandemic.

Social media users, who actively share deceptive content, exacerbate these problems, as they are acting as proxies for the producers of propaganda deceptions, multiplying the reach and footprint of the propagandists producing this content, especially if these social media users have large networks of followers.

Such social media users are typically cast as victims, which they often are, but every time such social media users share a falsehood they also become active participants in the propagandist's deception, or put bluntly *"proxy deceivers".*

As noted in an earlier submission to the federal Joint Standing Committee on Electoral Matters, the problems we now see with gullible social media users, public, and mass media falling for naïve or trivial deceptions will be immensely exacerbated as "deep fakes" become exploited for mischief and state sponsored propaganda. Deep fake technology was predicted two decades ago but largely ignored at the time, as its implications were neither appreciated nor understood[3].

[3] Refer Kopp, C., *Moore's Law and Its Implications for Information Warfare*, Proceedings of the International AOC Electronic Warfare Conference, Zurich, Switzerland, May, 2000. Deep fakes employ AI techniques to produce lifelike synthetic video and voice representations of individuals. Events or statements that never occurred can thus be produced.

Observations

The problems and consequent direct social and political impacts we are now observing in the COVID-19 / SARS-CoV-2 *"Deception Pandemic"* are not new, and have been well studied in recent years following the immensely disruptive foreign influence campaigns conducted to compromise the US 2016 Presidential Election, the UK Brexit vote, and a number of other votes in European nations.

More recently we are seeing reports of the same methods and tactics being reused or further enhanced to target the US 2020 presidential election.

Nearly all of the methods and tactics employed are digital evolutions of methods devised almost a century ago by *Soviet* and *Komintern* propagandists and applied extensively through the Cold War, with the caveat that during the Cold War the sought outcome was mostly to recruit supporters, while the currently sought outcome is mostly social disruption.

These campaigns produce effect primarily due to the gullibility or naïveté of large proportions of the target audiences of these campaigns, be it public or mass media[4].

Until both public and mass media are actively taught to recognize and reject propaganda narratives and deceptions, the problem will persist. Humans are naturally prone to accept narratives that align with their prior cognitive biases and deceptions crafted around these biases will often be accepted ahead of facts that do not confirm prior beliefs (there is extensive literature on this problem).

Simple refutations and fact checking can only "immunize" a victim audience against a single falsehood, unlike teaching victim audiences to be skeptical and critically assess what they are being presented with. This critical point is frequently ignored in the public debate on dealing with deceptions as teaching audiences to think critically and be skeptical is challenging and thus not amenable to simple and inexpensive solutions.

As noted in earlier submissions to the federal parliamentary JSCEM by this author and collaborators, there does not appear to be any *"silver bullet"* easy solution for defeating the problem of misinformation, disinformation and malinformation in social media, and the interconnected problem of such deceptions being spread in the mass media. Claims otherwise collide with decades of empirical observation that shows no evidence that any *"silver bullet"* solution exists.

It appears that the best approach may well be to appropriate ideas from traditional epidemiology, where a biological pathogen is actively interdicted along the whole

[4] The well known 2016 Stanford study by Wineburg et al showed that 80% of a student test population were challenged to recognize web content that was nonsensical, or contaminated with political or commercial bias. Other studies have shown similar problems in the adult population, even where the population in question was ostensibly well educated.

transmission chain, and the potential victims actively immunized. With a “digital pathogen” this means interdicting the flow of deceptive material from its source to its victims, and teaching the intended victims how to recognize and reject such deceptions. To implement such measures will require investment in capabilities, and investment in research to support these capabilities.

The risk for all democracies, if measures are not implemented to counter foreign nation state players using social and mass media to propagate falsehoods, is serious and ongoing disruption to the very fabric of all democratic societies subjected to such attacks.

The chaos and disruption observed as a result of the failure to effectively contain misinformation, disinformation and malinformation in social media, and mass media, during the current COVID-19 / SARS-CoV-2 pandemic, provides a good indication of the damage foreign nation state actors can inflict with a very modest investment.

Recommendations

Panacea Solutions: There is no sound evidence to support the proposition that *"one size fits all"* panacea solutions exist and any such proposals should be considered with proper caution.

Globalisation of Online Fakes: the global reach of digital media, encompassing the full gamut of digital channels the public has access to, makes every member of the public a potential target for foreign and domestic players propagating agendas that may be contrary to the national and public interest. The use of proxy entities to propagate fakery further exacerbates this problem. Attempts to divide responsibilities on the basis of state and federal jurisdictions should be considered with proper caution.

Regulatory Measures (1): claims that censorship in its various forms is an effective solution are poorly supported and may produce adverse impacts on freedom of speech and openness of public discourse, with the caveat that content which is harmful beyond dispute should be censored. Notably, nations with stringent censorship measures such as Russia or Iran have seen a large scale shift by users to encrypted messenger tools to bypass censorship mechanisms. Measures reliant on censorship should be thus considered with proper caution.

Regulatory Measures (2): *"fact checking"* measures in social media are often problematic, as fact checker bias or illiteracy may produce damage comparable to the fakery being fought. Measures reliant on *"fact checking"* should be considered but with proper caution.

Regulatory Measures (3): a variant of the now defunct US *"Fairness Doctrine"* in broadcast media could address many of the problems currently observed with bias in partisan mass media, but if misapplied would provide opportunities for foreign propagandists. Measures reliant on a "*Fairness Doctrine*" should be considered but with proper caution.

Primary and Secondary Education: Consideration should be given to amending the core curriculum of both primary and secondary education systems to include a very robust and formally assessed component addressing critical thinking skills and literacy in digital media deceptions.

Public Education (1): Consideration should be given to making literacy in digital media deceptions a compliance requirement for employers as false beliefs and uncertainty produced by false claims can adversely impact productivity and workplace safety (numerous examples can be observed in COVID-19 fakery).

Public Education (2): Consideration should be given to the provision of assessed free online courses to teach literacy in digital media deceptions, and the provision of a "*micro-credential*" on this topic.

Public Education (3): Consideration should be given to television and social media advertising on the risks and damage effects arising from uncritical acceptance of falsehoods being propagated via digital media. This is especially important for parts of the community who are less engaged online and more vulnerable to deceptions.

Public Education (4): Consideration should be given to television and social media advertising in foreign languages on the risks and damage effects arising from uncritical acceptance of falsehoods being propagated via digital media. Minorities who rely on foreign media rather than domestic media can be exposed to falsehoods via foreign media.

Media Education: Consideration should be given to making literacy in digital media deceptions a compliance requirement for all mass media providers resident in the state. There is ample evidence across the media that many media personnel are not well equipped to deal with this problem and effectively exacerbating the problem by careless spreading of deceptive content.

Public Communication: Public communication by government agencies in most Western democracies has been too frequently ineffective in dealing with deceptions in digital media. Consideration should be given to revising techniques and processes to improve both reaction times and effectiveness.

Research Capability: Australia lags leading OECD nations in the skills base required to deal with fakery in digital media. This is mostly a consequence of this research area not being robustly funded over the last two decades despite growing evidence of its importance. Consideration should be given to funding academic research to provide the skills sets to deal with the problem of deceptions in digital media. Options include research grant funding and PhD scholarship funding.

References:

1. Kopp C, Korb KB, Mills BI "Information-theoretic models of deception: Modelling cooperation and diffusion in populations exposed to 'fake news'". *PLOS ONE* 13(11), November, 2018: e0207383, URI: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0207383
2. Kopp, C, Korb, K.B, "We made deceptive robots to see why fake news spreads, and found its weakness", *The Conversation*, November, 2018, URI: https://theconversation.com/we-made-deceptive-robots-to-see-why-fake-news-spreads-and-found-a-weakness-104776
3. Kopp, C, Korb, K.B, Mills, B.I., "Understanding the Inner Workings of "Fake News"", *Science Trends*, November, 2018, URI: https://sciencetrends.com/understanding-the-inner-workings-of-fake-news/
4. Kopp, C., "*Understanding the Deception Pandemic*", Presentation Slides, Australian Skeptics Seminar, 16th July, 2018, Melbourne, Australia, URI: http://users.monash.edu/~ckopp/Presentations/Understanding-The-Deception-Pandemic-2018-B.pdf
5. Carlo Kopp, Kevin B. Korb, Bruce I. Mills, Written Evidence, "*Inquiry on Disinformation and 'fake news'*", House of Commons Digital, Culture, Media and Sport Committee, 12 December 2018, URI: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/written/93672.html
6. Carlo Kopp, Kevin B. Korb, Bruce I. Mills, *Dealing with the "Fake News" Problem*, Submission to the Joint Standing Committee on Electoral Matters, 17th January, 2019, URI: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/AECAnnualReport2017-18/Submissions
7. Kopp, C, *Fake news: The other pandemic that can prove deadly*, Expert Commentary, Monash Lens, URI: https://lens.monash.edu/2020/03/26/1379893/fake-news-the-other-pandemic-that-can-prove-deadly
8. Kopp, C, *COVID-19: Understanding – and misunderstanding – epidemic models*, Expert Commentary, Monash Lens, URI: https://lens.monash.edu/@carlo-kopp/2020/04/16/1380098/covid-19-understanding-and-misunderstanding-epidemiology-models
9. Seeme F., Green D., Kopp C.,*Pluralistic Ignorance: A Trade-Off Between Group-Conformity and Cognitive Dissonance.* In: Gedeon T., Wong K., Lee M. (eds) Neural Information Processing. ICONIP 2019. Lecture Notes in Computer Science, vol 11954. Springer, Cham. https://doi.org/10.1007/978-3-030-36711-4_58
10. Kopp C., "*Considerations on deception techniques used in political and product marketing*", Proceedings of the 7th Australian Information Warfare and Security Conference, 4 December 2006 to 5 December 2006, School of Computer Information Science, Edith Cowan University, Perth WA Australia, pp. 62-71. URI: http://users.monash.edu/~ckopp/InfoWar/Lectures/Deception-IWC7-2006-BA.pdf
11. Kopp C., "*Classical Deception Techniques and Perception Management vs. the Four Strategies of Information Warfare"*, in G Pye and M Warren (eds), Conference Proceedings of the 6th Australian Information Warfare & Security Conference (IWAR 2005), Geelong, VIC, Australia, School of Information Systems, Deakin University, Geelong, VIC, Australia, ISBN: 1 74156 028 4, pp 81-89. URI: http://users.monash.edu/~ckopp/InfoWar/Lectures/Deception-IWC6-05.pdf
12. Kopp C., "*The Analysis of Compound Information Warfare Strategies",* in G Pye and M Warren (eds), Conference Proceedings of the 6th Australian Information Warfare & Security Conference (IWAR 2005), Geelong, VIC, Australia, School of Information Systems, Deakin University, Geelong,

VIC, Australia, ISBN: 1 74156 028 4, pp 90-97. URI: http://users.monash.edu/~ckopp/InfoWar/Lectures/Method-IWC6-05.pdf

13. Kopp C., "*Shannon, Hypergames and Information Warfare*", in W Hutchinson (ed), Proceedings of the 4th Australian Information Warfare & Security Conference 2003 (IWAR 2003). Perth WA Australia, 28 - 29 November 2003, Edith Cowan University, Churchlands WA Australia, ISBN: 0-7298-0524-7. URI: http://users.monash.edu/~ckopp/InfoWar/Lectures/_JIW-2002-1-CK.pdf
14. Kopp C. and Mills B.I., *"Information Warfare and Evolution*", in W Hutchinson (ed), Proceedings of the 3rd Australian Information Warfare & Security Conference 2002 (IWAR 2002). Perth WA Australia, 28 - 29 November 2002, Edith Cowan University, Churchlands WA Australia, ISBN: 0-7298-0524-7, pp 352-360. URI: http://users.monash.edu/~ckopp/InfoWar/Lectures/_JIW-2002-2-CK-BIM.pdf
15. Yariv Tsfati, H. G. Boomgaarden, J. Strömbäck, R. Vliegenthart, A. Damstra & E. Lindgren (2020) Causes and consequences of mainstream media dissemination of fake news: literature review and synthesis, *Annals of the International Communication Association*, 44:2, 157-173, DOI: 10.1080/23808985.2020.1759443
16. Broniatowski, D.A., Jamison, A.M., Qi, S.H., Al Kulaib, L., Chen, T., Benton, A, Sandra C. Quinn, SC, and Dredze, M., Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate, *American Journal of Public Health* 108, 2018, 1378_1384, https://doi.org/10.2105/AJPH.2018.304567
17. Broad, W.J., Your 5G Phone Won't Hurt You. But Russia Wants You to Think Otherwise, *New York Times,* May 12, 2019, URI: https://www.nytimes.com/2019/05/12/science/5g-phone-safety-health-russia.html
18. Prothero, M., 5G coronavirus conspiracy theory that led to arson attacks on cell towers is being pushed by Russia, security officials fear, *Business Insider*, 17th April, 2020, URI: https://www.businessinsider.com/5g-coronavirus-arson-cellphone-towers-russia-iran-bots-2020-4
19. Graham, T., The story of #DanLiedPeopleDied: how a hashtag reveals Australia's 'information disorder' problem, *The Conversation*, August 14, 2020, URI: https://theconversation.com/the-story-of-danliedpeopledied-how-a-hashtag-reveals-australias-information-disorder-problem-144403
20. Kopp, C., *Moore's Law and Its Implications for Information Warfare*, Proceedings of the International AOC Electronic Warfare Conference, Zurich, Switzerland, May, 2000, URI: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.37.4257
21. Wineburg, Sam and McGrew, Sarah and Breakstone, Joel and Ortega, Teresa. (2016). *"Evaluating Information: The Cornerstone of Civic Online Reasoning.*" Stanford Digital Repository. Available at: http://purl.stanford.edu/fv751yt5934
22. Samantha Bradshaw, Lisa-Maria Neudert, Philip N. Howard, "COUNTERING THE MALICIOUS USE OF SOCIAL MEDIA: GOVERNMENT RESPONSES TO MALICIOUS USE OF SOCIAL MEDIA", NATO STRATCOM COE, Riga, November 2018, 11b Kalciema Iela, Riga LV1048, Latvia, URI: https://www.stratcomcoe.org/download/file/fid/79655

End of Submission