RESEARCH AND ANALYSIS

Hybrid CoE Trend Report 4

MAY 2020

Trends in the Contemporary Information Environment

HYBRID COE EXPERT POOL MEETING ON INFORMATION

Hybrid CoE

Hybrid CoE Trend Report 4

Trends in the Contemporary Information Environment

HYBRID COE EXPERT POOL MEETING ON INFORMATION

Hybrid CoE Trend Reports are an outcome of expert pool meetings on a given theme. They highlight the main trends of the theme, provide multiple perspectives on current challenges as well as academic discourse on the topic, and serve as background material for policymakers. They aim to distinguish between what really constitutes a threat, what appears to be a threat but is not necessarily one, and what has the potential to become one. Hybrid CoE's Research and Analysis engages expert pools on relevant themes in the landscape of hybrid threats.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-41-0
ISSN 2670-1804

May 2020

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland.

Contents

Foreword

The European security environment is becoming increasingly hybrid in nature. In addition to the traditional military domain, security threats are trickling down to all aspects of social life as democratic states encounter threats from actors who are willing and more able than ever before to attack domains not perceived to belong to the core field of security with multiple tools in a creative combination to achieve their goals and push their strategic interests in unacceptable ways.

Analyzing emerging trends related to security and highlighting long-term undercurrents will help us to understand the changing security environment and be better prepared to respond to potential hybrid threats in the future. Being able to read trends allows us to place current events into context, and helps us to distinguish between what is a threat, what looks like a threat but is not necessarily one, and what has the potential to become a threat in the future.

The European Centre of Excellence for Countering Hybrid Threats operates expert pools to support its participating states and the activities of the Centre's Communities of Interest. The expert pools work as a channel for exchanging information, building connections and gaining a comprehensive understanding of the trends under a specific theme.

These trends are then linked through Hybrid CoE to potential hybrid threats. The expert pools are an ongoing process and provide content for the Centre's work.

Engaging with the expert pools and the activity relating to them is in line with Hybrid CoE's founding memorandum of understanding, which states that Hybrid CoE is to act as a hub of expertise, to offer collective expertise and to encourage strategic-level dialogue. This activity should adopt a multidisciplinary and academic-based approach. Hence, the purpose of engaging with the expert pools is not to pursue a single truth, but rather to provide multiple perspectives on current challenges, to provide perspectives on the academic discourse on the topic, and to serve as a background for policymakers. The added value of this work is that it examines the subject from a hybrid threat perspective. Each participating state, the EU and NATO can then consider which facets of knowledge will be most useful for them from their own perspective.

This report is based on Hybrid CoE's Information Expert Pool's first meeting, which was held in Helsinki, Finland on 4–5 November 2019. The report has been compiled by Dr. Katerina Tsetsura together with Hybrid CoE Director of Research and Analysis Hanna Smith and Expert Pool Coordinator Emma Lappalainen.

Introduction

The media environment today is increasingly contested and rapidly changing. Geopolitical contestation, as well as an unregulated private media sector and domination by digital platforms, affect the content and quality of information. National information and the media space have become international and are being populated by a wide variety of actors. This new configuration of the information space presents new threats of political interference and influence from both states and non-state actors directed at countries abroad. In the era of hybrid threats, we have experienced profound changes to our security environment. The development of technology, social trends and geopolitical positions has led to a change in the relative effectiveness of the methods and given them new forms. This is also the case when it comes to the information domain, which is very often linked to different activities relating to hybrid threats as well as to priming for more serious action.

This report is based on expert written input from Hybrid CoE Information Expert Pool Members as well as discussions at the meeting held with multidisciplinary experts in Helsinki in November 2019. As a result, four trends were identified:
1. Fragmentation of the concept of truth,
2. Comprehensive changes of media as an industry 3. Hegemony of private media platforms and
4. New technologies that give rise to new tools for interference and influence. Each trend includes several sub-trends. By identifying the main sub-trends, it is possible to highlight key indicators for understanding the course of each trend.

1. Fragmentation of the concept of truth

A key component of the trend of the fragmentation of the concept of truth is that the notion of truth is increasingly contested. There is a plurality of narratives in a culture of individualization, increasing fragmentation, and disinformation. Furthermore, the increased inflow of information has created confusion between opinion, and journalistic, commercial, and politically loaded content.

The increasing amount of disinformation is shaping the information environment. Authoritarian states generate narratives to support their own strategic aims. For them, the emphasis on the individual will create wedges between civil societies and governments. The increased emphasis on the individual is seen in the fragmentation of media and of opinions, as well as in the polarization of politics. Disinformation, fragmentation, and polarization have resulted in a media ecosystem in which it is difficult to separate opinion, facts, and advertisements from one another. Additionally, efforts by authoritarian regimes to create enabling environments for the consumption of government-sponsored media contribute to contesting the concept of *truth*. There are also challenges in democratic societies that contribute to fragmentation and polarization. These challenges stem from both internal factors and external factors (hostile actors), and what these hostile actors do in their own countries. Therefore, the first trend, *Fragmentation of the concept of truth*, consists of three subtrends: 1) disinformation, 2) the construction of an enabling environment by authoritarian regimes, and 3) polarization and fragmentation.

1.1 Disinformation

The amount of disinformation derived from foreign actors is increasing. The structural causes are technological (related to the explosion of digital platforms, together with increasingly accessible affordances for content production, dissemination, and amplification) and geopolitical (competitive story-telling, shifting geopolitical realities, weaponization of information, loss of monopoly over the information space, and liberal overreach and counter-reactions to it).

The Kremlin is increasing its information aggression, to which end the budget for its main disinformation-oriented companies has grown by 30 per cent. This data is collected just through the official channels, so it is fair to assume that funding for the disinformation machine is significantly higher (Kalensky, 2019). The infamous troll factory in St Petersburg has been growing in past years, too, and recently the organization and other entities connected to it have been expanding their activities to Africa (see also here) and probably even Asia (Associated Press, 2019; Harding & Burke, 2019; Mackinnon, 2019).

In the Euro-Atlantic information space, both general audiences and decision-makers are becoming increasingly habituated to the prevalence and seeming inevitability of disinformation operations, which makes counteracting this new type of aggression significantly harder. This attitude is dangerous as it ignores the fact that disinformation is a strategic long-term game. As Giles (2019) has described, disinformation operations have varying levels of ambition. The fact that longer-term operations are less sensational and thus fall below the threshold of reaction does not mean that they are harmless. On the contrary, some opinion polls show that these operations have significant effects.[1]

Long-term disinformation campaigns, many of which demonstrate technological and psychological prowess, are based on a proven, pattern: repetition of a given message leads to familiarity, and familiarity leads to acceptance (Paul & Matthews, 2016). We see that the pro-Kremlin disinformation ecosystem consistently keeps repeating the same

[1] See articles in this reading list: https://euvsdisinfo.eu/reading-list/mechanisms/.

disinformation narratives (EUvsDisinfo, 2019). Accepting them as a new normal and as an inevitable part of our information environment is a clear win for the information aggressors. The second danger is that accepting some base level of disinformation operations as 'normal' will inevitably decrease the determination to counteract them, and to defend ourselves against this kind of information aggression. As a result, other actors are seeing that the West tolerates this type of aggression, and the number of actors using these weapons is duly on the rise. "Organized social media manipulation has more than doubled since 2017, with 70 countries using computational propaganda to manipulate public opinion," notes a recent study by the Oxford Internet Institute (2019). According to another study from Princeton University, Russia remains by far the most aggressive actor in terms of interfering in other countries' affairs, and is responsible for three times as many "foreign influence efforts" as all other actors combined (Martin & Shapiro, 2019).

At the same time, people are more confident in their ability to spot disinformation, but are actually less capable of doing so. The IPR Disinformation in Society report found that "four in five Americans (80%) feel at least 'somewhat' confident in their ability to recognize news or information that misrepresents reality or is false" (McCorkindale, 2019).[2] While this can be considered good news, it may also be signalling a **problem of overconfidence in our ability to detect fake news** or AI-generated audiovisual forgeries. Both under-confidence and over-confidence in an individual's skills in detecting fake content are problematic, and providing these individuals with critical thinking and basic fact-checking skills, and tools to recognize when one might be exposed to disinformation is critical to building societies that are resilient to information-influencing.

From the hybrid threat perspective, disinformation is part of priming the target, and building up the capabilities of the actor behind the disinformation. The coordination behind the repetition of a message is often difficult to detect and needs long-term monitoring in different languages and different geographical locations. This is one of the reasons why disinformation is a useful part of the toolkit in hybrid threat-related activity. Once priming has been carried out successfully, information campaigns can be activated in destabilization attempts. Therefore, all narratives in disinformation can subsequently be used in a more aggressive campaign. Disinformation continues to be one of the main sub-trends feeding into the trend of *Fragmentation of the concept of truth*.

1.2 Construction of an enabling environment by authoritarian regimes

Authoritarian regimes and actors that espouse authoritarian thinking are known to target democratic state systems with hybrid threat-related activity. The mechanism behind hybrid threats will not work unless the groundwork is well laid beforehand. Authoritarian regimes and actors play an important role in mediating the construction of cultural statecraft (history, culture, religion, language etc.) as an enabling environment to develop the context for actions taken by their governments. This construction happens in three specific ways (which can also be seen as challenges by the West): 1) a systematic effort to discredit traditional leading media that follow Western-based notions of objectivity in journalism and the presentation of at least two sides to every story; 2) a coordinated effort to build alternative mediated reality, through the support of carefully curated media; and 3) an organized effort to support language-specific initiatives to connect a specific culture to a specific country, as in the case of Russia connecting Russian cultural heritage with the country's position in the world as a leading actor (Tsetsura, 2020a).

The mediated construction of cultural statecraft is an increasingly active effort to engage Russian speakers and non-Russian speakers throughout Europe and the rest of the world in sharing the narratives constructed by Russia's mediated strategic communication efforts. This is performed through the systematic use of cultural statecraft strategies, combined with cultural diplomacy and the online process of development of what can be

[2] Among the social media platforms and according to the same report, YouTube is reported to have the higher score in terms of "trustworthiness as an information source" followed by Facebook.

called MDISS Information (Mediated Distraction In Shared Spaces) (Tsetsura, 2020b). Cultural statecraft allows for the building of an enabling environment (Klyueva & Tsetsura, 2015b) which facilitates the buying into the narrative of goodwill of Russia as a crusader against Western dominance in the world.

As a result of increasingly systematic work by the Russian government in addressing the requirement of the National Security Concept (2000) to secure the nation's presence in the global arena, the use of cultural statecraft-related tools to shape an enabling environment in multiple parts of the world has led to the creation of several networks for reaching wide audiences. First, a network for comprehensive online distraction and noise amplification and multiplication has been created and supported (a systematic effort to discredit the mainstream media). Second, a network of government-supported multimedia outlets, both inside and outside the country, is available in major spoken languages (a coordinated effort to build an alternative mediated reality). Third, the creation and support of the Russkiy Mir Foundation, which focuses on global cultural diplomacy efforts, is specifically built on the connection between contemporary Russia and the Russian language and the Russian Orthodox Church (an organized effort to support language-specific initiatives and culture-based activities). The Russkiy Mir Foundation (which translates as the Russian World Foundation), established by President Vladimir Putin and supported by the Ministry of Foreign Affairs and the Ministry of Education and Science, is a quasi-governmental institution that received both private and government funding (Blitt, 2011). In short, Russia might be organizing its efforts to affect those people who are open and susceptive to the Russian ideals.

This usage of cultural statecraft in an effort to shape an enabling environment where different networks are built to support the actors' strategic aims is not only practised by Russia. Several other authoritarian states have increased their efforts in building different networks and relying on different aspects of cultural statecraft. Furthermore, non-state actors are also becoming significant players in the field of disinformation and building networks based on cultural attraction. This might turn out to be an even bigger challenge in the future than an environment generated by authoritarian states. Hence, it can be argued that the sub-trend of constructing enabling environments is becoming increasingly prevalent.

1.3 Polarization and fragmentation

In democratic systems, we have viewed political polarization as a benefit for democracy as it mobilizes political participation, simplifies the political choice for voters, and strengthens political parties. The political sociological theory of democratic elitism by John Higley and his collaborators in the 1980s directed attention to the social and political preconditions of the stability of liberal democracies. They showed that the basis of the stability of a democratic regime is the forming of an underlying consensus among elites rather than among voters. While this consensus might not extend to values, it covers the norms that concern the operation of democratic institutions. If this consensus is not formed, or unravels, the stability of democracy is imperilled. In today's society, it seems that polarization, and fragmentation of both the societal and elite levels, are increasing in many countries and the different information environments. To this end, they are highlighted as important sub-trends of the identified trend.

To evaluate the extent of polarization, the public debate may be examined to gauge whether it is an inclusive one, and whether the problems that it addresses are those at the heart of the people and society. From the spirit and character of the public debate, we were able to deduce the degree of polarization and divisions and the weakening of society's defences from the absence of social cohesion. The divisions are deepening, but not along the traditional left-right lines. Today, we have globalist/cosmopolitan versus nationalist; religious versus secular; urban versus rural; traditional versus modern cultural values; and participatory versus representative democratic models, to name a few. These dividing lines are easier to assist from outside than traditional political ones. Internally born and homegrown polarization in a democratic society is not a threat, but if that process is intercepted by outside actors that see democratic systems as a threat to their own power, the situation changes radically and a threat emerges.

Digital media have served to intensify the trend of polarization and extreme opinions, and offer many avenues for outside intervention. Social media have bolstered "echo chambers", where people either knowingly or unknowingly choose information and groups with similar interests and mindsets and block out other opinions, arguably even leading to *tribal politics*.[3] It should be noted, however, that the notion of echo chambers has also been criticized by some scholars (see, for instance, Bruns' book *Are Filter Bubbles Real?*, Bruns, 2019b). When such a wide range of information is available, an individual can easily shut out certain channels and only follow those that correspond to their existing perception of the world – be it based on fact or opinion. This can also happen unwillingly, simply through the algorithms that recommend content to users based on what they have previously consumed, pointing to a cognitive vulnerability being created. For instance, a recent study found that Twitter users are, to a large degree, exposed to political opinions that align with their own (Merilainen-Tenhu, 2018).

Today, the problem is that the content is lacking for the user and, due to non-transparency, the media can also be accused of manipulation or of spreading strictly commercial news (Tsetsura & Kruckeberg, 2017). It is becoming increasingly difficult to detect manipulation. This deepens polarization and has resulted in decision-making problems. Studies have also shown that opinions and individuals have been targeted and manipulated by algorithms and bots to increase this polarization effect (see the Computational Propaganda Project, 2020).

Responding to the threat requires political consensus and cooperation at the elite level first and foremost. However, significant lobbying bodies aim at the contrary. Conservative Christian movements are tightening their networks and are directing significant amounts of funding into media operations that spread climate change denialism, disseminate hate speech against experts and journalists (females in particular), and are actively seeking collaboration with like-minded governments. In Estonia, for example, a strong polarizing discourse between Estonian speakers and Russian speakers is manifested in the narratives about WWII. The more the Russian-speaking population is targeted with such narratives, the more polarized the opinions become as they feel that an alternative identity is being created for them.

This all points to the fact that the distinction between fact and opinion is becoming blurred and we are facing a return of ideological media. This time, however, it is not clear what is ideological and what is not. As Pomerantsev (2019) argued, the belief that truth is out there if one looks for it hard enough has been replaced by an "ersatz reality", which works to extend the notion of subjectivity into all realms of knowledge. Living in an era when "nothing is true and everything is possible", as the title of another book by Pomerantsev (2015) declares, might be a new global reality for which the Western world needs to be well prepared. This does not necessarily mean that people would not value facts, but rather that an increasing number of citizens might be more susceptible to disinformation due to the compression of time and space in information distribution and verification. This is a fruitful terrain for hostile outside interference.

[3] Tribal politics means following a particular path of policies more associated with a political party dogma rather than the general good of the country and all of its people.

Issues and indicators for trend monitoring

Actors: How can disinformation by internal and external hostile actors be separated in detection?

Tactics and methods of disinformation: The familiarity of a message is a key factor in disinformation, and repetition leads to acceptance. How can patterns of repeated messages be recognized? Polarization and fragmentation research within a country will enable our understanding of potential vulnerable targets for disinformation operations.

Instruments and processes: Authoritarian regimes work meticulously to create enabling media environments for distributing strategic narratives. Cultural statecraft tools need to be monitored to understand how these enabling environments are being created.

Trends to watch: An increase in the plurality of narratives creates confusion and blurs the lines between news media and commercial, opinion-driven, and ideological content. How do internal and external hostile actors use this blurring line to their advantage? How does the compression of time and space affect citizens' ability to be critical towards media content?

2. Comprehensive changes of media as an industry

The second trend is the comprehensive change of media as an industry, reflected in the fact that we are living in a changing media and information ecosystem. As faith in traditional media institutions is fading, we might soon experience a version of a collapse of the expert system, with new loyalties being created to individuals and groups rather than to nation-states and supranational structures. This media and information ecosystem is being dominated by large digital platforms, whose domination has implications for the accessibility to and affordability of quality information, making it increasingly difficult to attribute sources of information, and to hold someone accountable. Interconnectivity through networks is increasing the speed and scope of information circulation and amplification, and visual discourse is now preferred at the expense of text. The media industry is becoming increasingly dominated by money flows and by an increasing number of state and non-state actors, as well as by influential individuals.

Television and the mainstream media in general are going online. Broadcasting via satellite and terrestrial digital broadcasting are becoming outdated. The future of broadcasting is via the internet. This means that the public will be even more exposed to all kinds of media content, and monitoring and limiting content may be challenging. Democracies can be challenged by fake news and disinformation content emanating from a wide range of sources.

One change in the media industry is consumers' increasing reliance on **visual information**, particularly among younger generations, and the increased use of big data-driven and algorithmic learning (machine learning and artificial intelligence) to identify, **manipulate**, and disseminate **(audio-)visual information**. A recent Reuters digital news report shows that visual platforms (such as Instagram) are increasingly relevant – particularly for young media users (Newman, Fletcher, Kalogeropoulos, & Nielsen, 2019), who are increasingly acquiring information via (audio-)visual media (vom Orde & Durner, 2019). The NGO Lie-detectors (www.lie-detectors.org) reported that younger consumers in particular are using visual media and are "barely [engaging] with the accompanying text" (Reppert-Bismarck, 2019, p. 9). The visualization of communication habits is also mirrored in the emergence of live-streamed terrorist attacks, such as those in 2019 in Christchurch, New Zealand, and Halle, Germany. It is likely that journalists (and possibly politicians) will increase their engagement with this visual and audio content.

There is clearly a generation gap. Younger generations seem to be quite good at spotting visual cues for "fakes" (Reppert-Bismarck, 2019, p. 9), but this might not be true of all generations and all intermediaries (namely politics and the media). Furthermore, an indirect effect might be the fuelling of distrust towards all visual content. There is a considerable risk that attempts to combat the spread of contaminated visual information – if employed rapidly – will fuel censorship, threaten artistic freedom, and contribute to even greater distrust among the public. But there are many ways in which democratic societies can combat this problem, without giving up their values (Kalensky, 2019). Hence, there is a need to foster individuals' democratic resilience.

The trend of this comprehensive change in the media industry has the following sub-trends: 1) financial flows, 2) diminishing quality of journalism, and 3) the emergence of new actors.

2.1 Financial flows

The financial flows of the media business industry are not always clear. Media monopolies on the one hand and government control (overt or covert) on the other create further challenges for independent media systems worldwide. Many journalists, particularly in authoritarian regimes, leave their jobs in fear of their lives or simply because they can no longer afford to support their families on a journalist's salary (Klyueva & Tsetsura, 2015a). Harsh economic conditions, as well as increasingly blurred lines between journalism and native advertising (sponsored content) in many countries around the world, often push journalists to work as freelancers. As a result, their work is funded by outside sources, either knowingly or unknowingly to the journalists themselves (Tsetsura & Kruckeberg, 2017). For example, the funding of private content creators who have their own YouTube or Instagram channels is difficult to trace. More broadly, media non-transparency is on the rise worldwide, and growing concerns about non-transparent media practices are being addressed by many groups (Tsetsura & Kruckeberg, 2017).

Furthermore, private firms finance content through new forms of hidden commercials, without regard for the values they are financing. Although discussions about ethical issues within native advertising are increasingly common among advertisers, large advertising firms, and media-related NGOs, such as initiatives by the Center for International Media Assistance, the Ethical Journalism Network, Omnicom, Procter & Gamble (Pritchard, 2020), and Reporters Without Borders, among others, disagreements still exist over who should establish guidelines and monitor the implementation of such guidelines.

2.2 Diminishing quality

The quality of journalism and news in general is suffering. Increasingly, news stories are being produced by individuals – bloggers, social media influencers and "citizen journalists" – who do not always have a background in journalism. Furthermore, funds for mainstream media are decreasing, leading to the media ecosystem being taken over by foreign media outlets and social media platforms, which has allowed authoritarian media giants to gain access. Content suffers when news content is produced by a wider variety of actors, such as bloggers and live streamers. Increasingly, quality content is only available behind a paywall, discouraging a mass audience from reading it when free content is available. Eventually, as mainstream journalism loses its market share, less of it will be available because rigorous journalism requires resources to have a sustainable business model in order to be financially sustainable. A base level of subscribers must be maintained, even if not everybody can afford access to verified hard news stories and analyses that are produced by reputable media outlets.

2.3 New actors

Big media corporations and digital platforms are taking over and are likely to exert a significant influence over global media trends. These platforms are not the ones that define the content, but their business models, data collection and personalization functions influence which content circulates the most and gains the most amplification and impact. As such, they might become the creators and providers of common narratives for millions of people. Such influence will have a particular impact on small open-democratic countries, although similar trends are also seen in large, established democracies, such as the United States. Local media might no longer be able to compete with big corporations and platforms, creating an opportunity gap in the creation and distribution of narratives among the public. Authoritarian regimes will certainly try to fill this gap with their own narratives (Sputnik and international variants of *China Daily* are good examples) (Filipova & Galev, 2018).

It is likely that new US players, such as Netflix and Amazon, may soon dominate the global entertainment landscape. They will create global narratives for a very narrowly targeted yet wide scope of audiences. Although Netflix and Amazon are focused on entertainment and not news media per se, other media players are taking note of how to combine entertainment value with news delivery. In global news distribution, undemocratic regimes might be actively present in the media field. They are presented through media that are portrayed as being independent but that are fully funded and connected to authoritarian states for the purpose of serving their strategic interests. For instance, Sputnik provides information in different local languages and, in the eyes of local audiences in small countries, it might be regarded as a legitimate source of information (Rutenberg, 2017). Some populations may be more susceptible to Russian information operations than others. RT's efforts are not limited to Western states (Kalensky, 2020). For example, in Central Asia and in the US, RT is widely accessible and is seen as a source of information (Rutenberg, 2017). Both Sputnik and RT serve the Russian state.

However, not all Russian actors in the media space should be labelled as state propaganda or fake news. The development of Russian civil society and the strengthening of democratic values within Russia are very weak but worth noting, although the hope that they might eventually reduce the Kremlin's dominance in the Russian information environment should not be high (Kalensky, 2019). An immediate implication for the West is that it is necessary to distinguish between different Russian information sources, one being media under the control of the political regime, and the other, albeit small, being the opposition to that regime, providing high-quality media content. These two information sources have different impacts on the information environment in EU/NATO member states. The Kremlin's controlled media influence largely has a strategic aim to advance Russia's strategic interests by all ways and means and to ensure that democratic countries are seen as being intent upon hurting Russia and trying to cover up their own weaknesses. Therefore the feeble independent media in Russia might have a limited but positive impact on the promotion of democratic values, countering the Kremlin's influence among local and global Russian-speaking audiences (Free Press Unlimited, 2020).

Issues and indicators for trend monitoring

Fading transparency of the media industry: What gaps, uncertainties, and weaknesses do hostile actors use in the changing media landscape?

Rise in media non-transparency: Media monopolies, government control, and blurring lines between journalism and native advertising are growing. How can governments create initiatives to combat disinformation within the blurring lines of disinformation and native advertising?

Diminishing quality: How do hostile actors exploit the trend of a decrease in quality journalism? Are individual bloggers, social media influencers and "citizen journalists" being harnessed for strategic purposes?

Competition opens up influence gaps: Big media corporations and digital platforms are taking over the local media space, opening it up to information operations by hostile actors.

Trends to watch: Faith in traditional media institutions is waning. The domination of the media environment by large digital platforms makes it increasingly difficult to attribute the sources of information, and accountability duly becomes more difficult. How effective are hostile states in exploiting this difficulty?

3. Hegemony of private media platforms

Private digital platforms are becoming increasingly powerful in the information ecosystem. However, companies such as Facebook, Twitter and YouTube have continually been criticized for not doing enough to prevent harmful content on their platforms (Cassidy, 2016; Dwoskin, Whalen, & Cabato, 2019). Additionally, they have been criticized for not being accountable and transparent in their operations (Frenkel et al., 2018). New regulations must be developed to enable transparency and accountability. New digital media platforms are growing in size and becoming prevalent platforms for sharing and disseminating news. Sharing news has become as important as producing it, because sharing of this sort is a sign of belonging to a certain group. Mainstream media still contribute to the distribution and dissemination of information, but this task is increasingly being taken over by individuals on digital platforms. Thus, the transfer of advertising money from mainstream media to digital platforms has taken place. In addition to news outlets, contemporary digital users also create the content. Anyone can be followed, and anyone's information can easily be shared. This third trend of the *Hegemony of private media platforms* has two sub-trends: 1) a power shift to individuals and micro-influencers, and 2) regulation challenges**.**

3.1 Power shift to individuals and micro-influencers

Today, influence does not necessitate working for a credible agency or having a proper education. Anyone can become influential on social media by providing content that meets the needs of the public. Anyone can become an influencer, even an avatar figure or someone who does not exist in reality (e.g. Lil Miquela, a fictional digital character, who is a Brazilian-American model and singer and a popular Instagram influencer with almost 2 million followers, created by a digital marketing agency). Power is increasingly shifting to micro-influencers, while social media influencers are not as identifiable and relatable. Some influencers are also establishing independent platforms to reach their audiences. Actors using smaller, independent platforms are also more difficult to investigate, including the transparency of their financial background and motives. Moreover, micro-influencers often use visual materials and other elements that are difficult to investigate. For instance, humour is something that is difficult to fact-check, but is very powerful. An individual can feel a sense of belonging by identifying with a group that gets the same jokes. Even if used by an outside actor for political or malign purposes, humour can easily be brushed off as "only humour", despite having a significant effect on the target audience.

3.2 Regulation challenges

It can be increasingly difficult to hold private and powerful actors accountable. Social media platforms have launched vague research initiatives that have been heavily criticized for merely paying lip service to resolving the problem (Salim, 2019). More openness should be demanded of social media, for example in its use of algorithms and its grounds for blocking certain content or accounts, but not others. Although social media companies have a vested interest in appearing to be "tough" on orchestrated disinformation campaigns, as in November 2019 when Facebook announced that they had removed 5.4 billion fake accounts during 2019 (Fung & Garcia, 2019), they also have a clear economic stake in limiting independent investigations that could result in bad press.

Twitter and Facebook have launched highly selective and limited initiatives that insufficiently address the need for investigation, and that have insufficient independence from the companies (Bruns, 2019). On top of this, Social Science One, a Facebook collaborator on the initiative to investigate the effect of social media on democracy and elections, recently threatened to pull out of the project because of repeated delays from the company (Bruns, 2018). Journalists in the USA have expressed deep frustration with Facebook's unwillingness to cooperate transparently (Levin, 2018). Moreover, although it is possible to succeed in influencing Western companies to take some measures to curb the spread of disinformation, there are also companies, such as TikTok (which originated in China), or Telegram (which is based in Russia and has considerable regional importance in the post-Soviet space), that might not yield to such pressures. The recent election in Taiwan serves as a timely reminder about the other possibilities that hostile actors have besides Facebook (or similar platforms) (Stop Fake, 2020). Overall, the threat of disinformation campaigns and foreign interference has only grown in recent years.

In response to scandals surrounding Cambridge Analytica and the Russian Internet Research Agency, tech firms have closed down their APIs (Application Program Interfaces) to external developers, including researchers and journalists. While the now-closed APIs were never ideal for research (Venturini & Rogers, 2019), scholars argue that their disappearance, with no alternatives in place, will severely limit future research about topics such as computational propaganda, while not substantially addressing the privacy concerns that the companies claim to mitigate (Bastos & Walker, 2018; Bruns, 2019a). Independent research is sorely needed, and scholars are realizing that legislation might be the only way to ensure it. Rather than enabling more investigative work by scholars and journalists, social media companies have increasingly limited the opportunities for studying their platforms, despite growing global threats from propaganda operations (Bradshaw & Howard, 2019). At the same time as social media platforms are gaining more influence, they are also avoiding responsibility and accountability. Selling media space to those who pay the price, regardless of what the content is, might not be the best practice for achieving transparency. Social media are currently restricting investigations into their activities, thereby reducing transparency (Kang & McCabe, 2019).

Issues and indicators for trend monitoring

Actors: *Private digital platforms* are key actors in the information ecosystem, especially in the prevention of harmful content on their platforms.

Microlevel-influencers provide content that appeals to audiences' needs, and anyone can become an influencer today. Micro-influencers are also starting their own independent media platforms. How can financial disclosure and all of the motives of micro-influencers be made transparent?

Transparency and accountability: How can liberal democratic states collaborate with large and micro-level private digital platforms to develop regulations on transparency and accountability that match the requirements of the traditional news media? What will the future of news media look like?

Trends to watch: The increasing number of micro-influencers increases the amount of personalized information-sharing. At the same time, it becomes more difficult to be assured of the transparency of information. Can hostile actors use micro-influencers to disseminate their narratives? How can liberal democracies collaborate with micro-influencers – and should they?

4. New technologies that give rise to new tools for interference and influence

Digital technology and the production, distribution, and amplification of content are more widely available than ever, and are advancing more rapidly than before. Such **"democratization" of digital communication technology means that the creation of high-quality or semi-professional digital audio-visual content**, developments in **artificial intelligence** for the generation of fake news articles[4] and audiovisual forgeries, and the possibility of rapidly **disseminating content through social media and live-streaming platforms** for virtually anybody with some basic digital skills are the new reality. Coupled with the growing hegemony of digital media in the information space, trans-Atlantic populations will be increasingly vulnerable to targeted hostile communication campaigns. Digital channels have emerged as a reserve for the collection of data and information on individuals that can be used for micro-targeting, either for commercial use or as planned, targeted influence communication campaigns by a hostile actor. Such micro-targeting further complicates the transparency of news and the information flow and can be used to circulate disinformation and deepfakes. Therefore, the fourth and final trend analysed is *New technologies that give rise to new tools for interference and influence*. The trend highlights two sub-trends: 1) cheap fakes and deepfakes, and 2) micro-targeting.

4.1 Cheap fakes and deepfakes

Deepfakes are a rather new but nonetheless prominent threat. The fear is that deepfakes will revolutionize deception and fake news, destroying the credibility of news organizations and manipulating elections. The term deepfake is usually associated with technologies that can manipulate video so that someone appears to be saying or doing things they have never said or done. Thus far, the quality of these fakes is, at best, mediocre and easy to spot; however, some high-end fakes are already available.

Today, many journalists would say "no video, no story", regarding video as an essential part of any news story, just as photographs used to be. Photographs have long been manipulated, a tactic that became widespread in Soviet times (Blakemore, 2018); however, society in general was aware of this and dealt with it accordingly. Why then are we unable to handle video manipulation in the same way, especially when we consider – as some correctly claim – that video is more influential?

Currently, we have little experience with fake videos although the number of manipulated photos and videos doubled in 2019 (Morris, 2019). A video featuring a slow-motion Nancy Pelosi recently drew much attention, but was quickly debunked (Harwell, 2019). We could draw a comparison with other fakes, such as fake or manipulated emails or messages. When someone hijacked AP's account and tweeted that President Obama had been wounded in an attack on the White House, the US stock market immediately lost 136 billon USD in value (More & Roberts, 2013). That attack lasted for seven minutes before it was corrected. If a video of an important person, say a head of state, appears with controversial content, how long will it take for the target to issue a correction or for analysts to technically reveal the manipulation? It is difficult to see how fake videos could be misused long enough to influence an election or otherwise help someone gain political influence.

Information ambushes have been used for political purposes even without deepfakes. In 2017, for example, someone hacked into the account of the Qatari news agency and issued statements supportive of Israel and Iran, which Qatar's neighbours used as a pretext for isolating

[4] See: https://grover.allenai.org.

the country (*The Telegraph*, 2017, May 24). Qatar's ambassador to Washington was also hacked and emails quoted in support of the story (Ahmed, 2017). Some years earlier, in 2008, Russia invaded parts of Georgia, cut off telecommunications, conducted Distributed Denial-of-Service (DoS) attacks on key mail accounts and websites, and flooded the world with claims of Georgian violence and atrocities (Karlsen, 2016).

These are cases of what can be described as an *information ambush*, in which manipulated information is used to move fast-forward, make an excuse for certain action, and create a fait accompli. Such manipulation can use all sorts of fakes and hacks, and deepfakes will certainly be another useful option. However, it is unlikely that deepfakes, if they have any importance, will survive scrutiny for long. Recent efforts against the use of deepfakes are promising (Morris, 2019) so it would appear that they are not in a position to change the course of elections, at least for now. However, the information domain has fostered tremendous creativity through the use of technology and once one form or format has been effectively detected or countered, the trend has been for new forms to emerge. One of the new formats could be audio fakes, which are easy to produce and harder to verify than video material.

4.2 Micro-targeting

Also referred to as "micro-targeting", "narrowcasting", "hypertargeting" and "pinpoint propaganda", the proliferation of the Internet of Things (IoT) – together with developments in online big data surveillance and behaviour-tracking, artificial intelligence (AI), and machine learning (ML) – is supporting the emergence of highly-targeted information operations, or what can best be described as *hyper-personalized influence targeting* (HPIT), to achieve not only military and geopolitical objectives, but also commercial, electoral, political and civic aims. Components of this technology have already been employed with varying degrees of sophistication and success in Ukraine, Syria, the US, the UK, and China.

For example, during the 2014 Maidan protests in Kiev and along the line of demarcation in eastern Ukraine (2014 to present), Russian forces have combined traditional electronic warfare (EW) equipment, commercial drone (UAV) technology, and/or IMSI-catchers (mobile cell tower imitators) with psychological operations and social engineering techniques to target and intimidate civilians, as well as to undermine soldier morale by surreptitiously sending inflammatory messages and facilitating kinetic/lethal targeting. Similar methods and technology have been employed by government forces in Syria to send SMS text messages to both the civilian population and the Syrian Democratic Forces (SDF) in specific geographic locations (nationwide dissemination), while the Chinese government has used targeted, paid advertisements on Twitter – directed towards a specific set of potentially influential users – to shape the perceptions of international audiences (the Hong Kong protests) (Lauder, 2019; Wood, 2019; Doffman, 2019; Williams, 2016). In one of the most sophisticated information campaigns, Cambridge Analytica – a private political consultancy working on behalf of various political organizations and lobby groups – employed advanced data-mining and analysis techniques with psychometrics and relatively new psychological profiling techniques, based on the 'big five' (OCEAN) personality index, to amplify and reinforce attitudinal preferences and to solidify favoured voting behaviour (US presidential elections, and Brexit). Similar, albeit less sophisticated, techniques were employed by the Internet Research Agency (IRA), a private media firm operating on behalf of the Russian government, to send inflammatory messages via Facebook, Twitter, and Instagram (and other social media platforms) to US citizens leading up to and during the 2016 presidential campaign, largely in an attempt to amplify social discontent, provoke violence, and undermine the electoral process (Thompson & Lapowsky, 2018). However, rather than being the pinnacle or the quintessence of influence, these examples merely represent an early stage of the technological and social scientific evolution of HPIT. It is posited that future applications of HPIT will be much more nefarious and insidious, and hence **difficult to identify and to counter**.

Hyper-personalized influence targeting has significant disruptive potential for the EU and NATO and their member states for several reasons. First, due to its relatively low cost, it is anticipated that the technology underpinning HPIT will be accessible to both state and non-state adversaries, or the technology will be available via lease agreements as a "service package" offered by third parties, such as commercial entities (for example, political consultants and public relations companies). Second, advancements in AI, as well as psychometrics and the underpinning psychological and sociological models, will enhance both the accuracy and efficacy of the message. In other words, the campaigns will be individually tailored and will duly have a high degree of resonance and affect. Third, advancements in this technology will allow hostile actors to design and conduct HPITs on an industrial scale – essentially fusing, or at least blurring, the traditional conceptual divide between the tactical and strategic levels. In other words, vast target audiences will be bombarded with individualized messaging (that is, tactical psy-ops meets strategic communications). Finally, it is expected that HPIT will be employed most often by hostile actors under the threshold of war, or what is often referred to as *Phase 0 operations* or *grey zone conflict*, to essentially exploit an area of the spectrum of conflict in which Western governments currently lack the policies, political will, and organizational structures and capabilities to both sense the *information attack* and to respond appropriately. As a result, target audiences residing in Western countries might remain vulnerable to exploitation by hostile actors, and Western countries may be helpless, or at least limited in their ability, to respond effectively.

Targets of manipulation can be examined on the macro level of societies (such as the media and governments), on the level of social groups (including extremists), and individual users. Fabricated or contaminated visual information can be intended to distort perceived public opinions (including indirect manipulations via "source hacking" journalists or politicians) (Donovan & Friedberg, 2019), to enhance tensions between social groups, to weaken societal cohesion (such as hateful memes rooted in fringe web communities) (Zannettou et al., 2018), or even to micro-target individuals for political purposes.

Issues and indicators for trend monitoring

Leveraging new technology: The number of photo and video manipulation examples is rising. How will hostile actors use AI and other technological advances to make manipulations appear more authentic? How can we detect cheap fakes and deepfakes?

Ambush: Information ambushes are used as a tactic for making an excuse for action. How can information ambushes be detected and deterred?

Micro-targeting: How can nation states gain knowledge early on of hyper-personalized influence operations?

Trends to watch: Macro-, social group- and individual citizen-level target analysis of hostile actors.

Conclusion

This trend report on the contemporary information environment has taken a closer look at four trends that emerged during discussions at the Hybrid CoE Information Expert Pool meeting in November 2019. The trends are: 1) Fragmentation of the concept of truth, especially as it relates to social trends and new ways in which information flows; 2) Comprehensive changes in the media as an industry; 3) The increasing hegemony of private media platforms that now compete with outlets, which are still referred to as the traditional media; and 4) New technologies that give rise to new tools for interference and influence. These trends are key features of Disinformation η.0 and are a confluence of the human contribution (that is, tailoring strategic messages and perceived ownership of shared messages) and the digital technology that is used to produce and amplify it. The resulting flow of content is neither true nor false in its entirety, but is merely algorithmic, big data-driven, continuously multiplying and morphing, and thus, ultimately, evading the control of its original source. It also builds on the efficient monetization of users' engagement, attention, and emotions (economies of attention).

We are currently living, communicating, and making decisions in **a completely new information and media environment** in which disinformation has become a **continuous** and **diffuse** process. This disinformation structure is rapidly developing and is improving as we speak (hence, we do not call it Disinformation 2.0 or Disinformation 3.0, 4.0. and so on – but rather, Disinformation η.0).

From the hybrid threat perspective, Disinformation η.0 is a confusing mix of strategic messages stemming from state and non-state actors (frequently disguised and hard to attribute) that consider the democratic state system to pose a threat to them. It is combined with advertising from commercial entities and mis- and dis-information that is disseminated by aware or unaware regular users. In this environment, the conflicts of popularity and perceptions are beginning to merge with real-life conflicts and divisiveness (Singer & Brooking, 2018), leading to increased online and offline polarization on social, economic and ideological grounds. In fact, online and offline instances of polarization crucially feed each other toward a point of no return to rational debate – "a paradise not just for fake news but also for extreme views" (Ferguson, 2017), and a binary world in which there is little room for ambivalence. When outside actors with the mentality to undermine and hurt the target start to use this information domain's "paradise", an unhealthy polarization occurs that can lead in the worst case to the destabilization of a state. This unhealthy polarization creates an "us versus them" mentality (Bremmer, 2018) that **amplifies engagement with politically-biased fake news**, exacerbates **negative emotions,** and leads to a generalized zeitgeist of **indignation and suspicion**, in which the sensational coverage of deepfakes makes even real news seem fake. This **generalized spread of confusion** hinders healthy debate in society and negatively affects governing and decision-making processes, as well as security and diplomacy.

List of contributors

Rubén Arcos, Lecturer at King Juan Carlos University, Spain

Alina Bargaoanu, Professor and Dean of the College of Communication and Public Relations, National University of Political Studies and Public Administration (Romanian School of Government), Romania.

Ieva Berzina, Senior Researcher**,** Center for Security and Strategic Research**,** National Academy of Defence of the Republic of Latvia

Christophoros Christophorou, Independent consult, Cyprus

Johan Farkas, PhD student, Media and Communication Studies, Malmö University, Sweden

Lena Frischlich, Research group leader, Institute for Communication Studies, University Muenster, Germany

Ivo Juurvee, Head of Security & Resilience Programme, International Centre for Defence And Security, Estonia

Jakub Kalensky, Senior Fellow, Digital Forensic Research Lab, Czech Republic

Geir Hågen Karlsen, Director for Strategic Communication at the Norwegian Defense University College, Norway

Emma Lappalainen, Expert Pool Coordinator, European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE

Matthew A. Lauder, Defence Scientist, Psychological Effects Team, Joint Targeting Section Defence R&D Canada

Mantas Maritsius, Chairman, Radio and Television Commission of Lithuania

Hanna Smith, Director of Research and Strategic Analysis function, European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE

Katja Valaskivi, Associate Professor, University of Helsinki, Finland

References

Ahmed, A. S. (2017, June 6). Someone is using these leaked emails to embarrass Washington's most powerful ambassador. *Huffington Post*. https://www.huffpost.com/entry/otaiba-ambassador-uae-leaked-emails_n_5932bf04e4b02478cb9bec1c?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLm5vLw&guce_referrer_sig=AQAAAAzpDQ9QX1oPff9pAE7cg46nqG0Onfl8Ln5J51XN5Iq9XcKZFdG-iwHQcIS32rzHUHdXt9S8tdsSWysKn9_yCd-AYM1eWIlYJH-QocojOxgL3FhTX641aNgf_EqpBk8WbH9QaKMik27oelX_D-Bor1ad6bOkz4_xdvxgkMJFjtBC.&guccounter=2.

Andrae, A. (2019). Prediction studies of electricity use of global computing in 2030. *International Journal of Science and Engineering Investigations (IJSEI)*, *8*(86), 27–33.

Associated Press (2019, January 17). *Facebook shuts hundreds of Russia-linked pages, accounts*. CBC. https://www.cbc.ca/news/technology/facebook-russiafake-news-1.4981734.

Bastos, M. T., & Walker, S. T. (2018, April 11). Facebook's data lockdown is a disaster for academic researchers. *The Conversation*. https://theconversation.com/facebooks-data-lockdown-is-a-disaster-for-academic-researchers-94533.

Blakemore, E. (2018, April 20). How photos became a weapon in Stalin's great purge. *History*. https://www.history.com/news/josef-stalin-great-purge-photo-retouching.

Blitt, R. (2011). Russia's "Orthodox" foreign policy: The growing influence of the Russian Orthodox Church in shaping Russia's policies abroad. *University of Pennsylvania Journal of International Law*, *363*, 1–60.

Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 Global Inventory of Organised Social Media Manipulation*. Research report. https://comprop.oii.ox.ac.uk/research/cybertroops2019/.

Bremmer, I. (2018). *Us vs. Them: The failure of globalism*. New York, NY: Penguin Publishing group.

Bruns, A. (2018). Facebook Shuts the Gate after the Horse Has Bolted, and Hurts Real Research in the Process. *Medium*, *28*, 449–461. https://doi.org/10.1046/j.1365-2958.1998.00797.x.

Bruns, A. (2019a). After the "APIcalypse": Social media platforms and their fight against critical scholarly research. *Information Communication and Society*, *22*(11), 1544–1566. https://doi.org/10.1080/1369118X.2019.1637447.

Burns, A. (2019b). *Are filter bubbles real?* Cambridge, UK: Polity Press.

Cassidy, A. (2016, August 26). Are Facebook and Twitter doing enough to protect users? *The Guardian*. https://www.theguardian.com/media-network/2016/aug/26/social-media-sites-protect-users-twitter-facebook.

Center for International Media Assistance (CIMA) (2020). Official website. https://www.cima.ned.org/.

Doffman, Z. (2019, August 19). China pays Twitter to promote propaganda attacks on Hong Kong protesters. *Forbes*. https://www.forbes.com/sites/zakdoffman/2019/08/19/twitter-under-fire-for-running-chinese-ads-attacking-hong-kong-protesters/#697db91c1f18.

Donovan, J., & Friedberg, B. (2019). *Source hacking – Media manipulation in practice*. Report. Data & Society Research Institute. https://datasociety.net/output/source-hacking-media-manipulation-in-practice/.

Dwoskin, E., Whalen, J., & Cabato, R. (2019, July 25). Content moderators at YouTube, Facebook and Twitter see the worst of the web – and suffer silently. *The Washington Post*. https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-price/.

Ethical Journalism Network (2020). Official website. https://ethicaljournalismnetwork.org/.

EUvsDisinfo (2019). *Pro-Kremlin disinfo cases*. Online database. https://euvsdisinfo.eu/disinformation-cases/.

Ferguson, N. (2017). *Speak less softly but do not forget the big stick*. Online post. http://www.niallferguson.com/journalism/politics/speak-less-softly-but-do-not-forget-the-big-stick-niall-ferguson.

Filipova, R., & Galev, T. (2018). *Russian influence in the media sectors of the Black Sea countries: Tools, narratives and policy options for building resistance*. Report. Center for the Study of Democracy. https://csd.bg/publications/publication/russian-influence-in-the-media-sectors-of-the-black-sea-countries-tools-narratives-and-policy-opti/.

Free Press Unlimited (2020). *Russian language news exchange supports independent media*. Online post. https://www.freepressunlimited.org/en/projects/russian-language-news-exchange-supports-independent-media.

Frenkel, S., Confessore, N., Kang, C., Rosenberg, M., & Nicas, J. (2018, November 14). Delay, deny and deflect: How Facebook leaders fought through crisis. *New York Times*. https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html.

Fung, B. & Garcia, A. (2019, November 13). Facebook has shut down 5.4 billion fake accounts this year. *CNN*. https://edition.cnn.com/2019/11/13/tech/facebook-fake-accounts/index.html.

Giles, K. (2019). *Moscow rules: What drives Russia to confront the West*. (The Chatham House Insights Series). Washington D.C.: Brookings Institution Press.

Harding, L., & Burke, J. (2019, June 11). Leaked documents reveal Russian effort to exert influence in Africa. *The Guardian*. https://www.theguardian.com/world/2019/jun/11/leaked-documents-reveal-russian-effort-to-exert-influencein-africa.

Harwell, D. (2019, May 23). Faked Pelosi videos, slowed to make her appear drunk, spread across social media. *The Washington Post*. https://www.washingtonpost.com/technology/2019/05/23/faked-pelosi-videos-slowed-make-her-appear-drunk-spread-across-social-media/.

Kalensky, J. (2019, July 16). Testimony for the Foreign Affairs Subcommittee on Europe, Eurasia, Energy, and the Environment. *DisinfoPortal*. https://disinfoportal.org/testimony-jakub-kalensky.

Kalensky, J. (2020, Jan. 8). *Russian disinformation in 2019: Review*. Online post. https://disinfoportal.org/russian-disinformation-in-2019-review/.

Kang, C., & McCabe, D. (2019, Nov. 6). California sues Facebook for documents in privacy investigations. *New York Times*. https://www.nytimes.com/2019/11/06/technology/facebook-california-investigation.html.

Karlsen, G. H. (2016). Tools of Russian influence: Information and propaganda. In J. H. Matlary & T. Heier (Eds.) *Ukraine and beyond: Russia's strategic security challenge to Europe* (pp. 181–208). London, UK: Palgrave MacMillan.

Klyueva, A., & Tsetsura, K. (2015a). Economic foundations of morality: Questions of transparency and ethics in Russian journalism. *Central European Journal of Communication*, *8*(1). http://ptks.pl/cejc/wp-content/uploads/2013/12/03-kluyeva.pdf.

Klyueva, A., & Tsetsura, K. (2015b). Strategic aspects of Russia's cultural diplomacy in Europe:

Challenges and opportunities of the 21st Century. In A. Catellani, R. Tench, & A. Zerfass (Eds.), *Communication ethics in a connected world: Research in public relations and organizational communication; EURPERA annual volume* (pp.175–198). Brussels: P.I.E. Peter Lang.

Lauder, M. A. (2019). Limits of control: Examining the employment of proxies by the Russian Federation in political warfare. *Journal of Future Conflict, 1*. https://www.queensu.ca/psychology/research/journal-future-conflict/journal-future-conflict-issue-01-fall-2019.

Levin, S. (2018, December 13). "They don't care": Facebook factchecking in disarray as journalists push to cut ties. *The Guardian*. https://www.theguardian.com/technology/2018/dec/13/they-dont-care-facebook-fact-checking-in-disarray-as-journalists-push-to-cut-ties.

Mackinnon, A. (2019, July 10). The evolution of a Russian troll. *Foreign Policy*. https://foreignpolicy.com/2019/07/10/theevolution-of-a-russian-troll-russia-libya-detained-tripoli/.

Martin, D. A., & Shapiro, J. N. (2019). *Trends in online foreign influence efforts*. Princeton ESOC Publications. https://esoc.princeton.edu/files/trends-online-foreign-influence-efforts.

McCorkindale, T. (2019). *2019 IPR disinformation in society report*. Institute for Public Relations, USA. Online report. https://instituteforpr.org/ipr-disinformation-study/.

More, H., & Roberts, D. (2013, April 23). AP twitter hack causes panic on Wall Street and sends Dow plunging. *The Guardian*. https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.

Merilainen-Tenhu, M. (2018, April 26). *Are social media echo chambers?* Press release. Aalto University. https://www.helsinki.fi/en/news/data-science-news/are-social-media-echo-chambers.

Morris, B. (2019, November 22). Tech companies step up fight against "deep fakes". *Wall Street Journal*. https://www.wsj.com/articles/tech-companies-step-up-fight-against-deepfakes-11574427345.

Newman, N., Fletcher, R., Kalogeropoulos, A., & Nielsen, R. K. (2019). *Reuters Institute Digital News Report 2019*. https://doi.org/10.2139/ssrn.2619576.

Oxford Internet Institute (2019). *Use of social media to manipulate public opinion now a global problem, says new report*. Press release. https://www.oii.ox.ac.uk/news/releases/use-of-social-media-to-manipulate-public-opinion-now-a-global-problem-says-new-report/.

Paul, C., & Matthews, M. (2016). *The Russian "firehouse or falsehood" propaganda model: Why it might work and options to counter it*. RAND online report. https://www.rand.org/pubs/perspectives/PE198.html.

Pomerantsev, P. (2015). *Nothing is true and everything is possible: The surreal heart of the new Russia*. New York, NY: Public Affairs. Hachette Book Group.

Pomerantsev, P. (2019). *This is not propaganda: Adventures in the war against reality*. New York, NY: Public Affairs. Hachette Book Group.

Pritchard, M. (2020, Jan. 15). *It's time to build a responsible media supply chain*. Opinion by M. Pritchard, CEO of Procter & Gamble. World Economic Forum. Official website. https://www.weforum.org/agenda/2020/01/time-to-build-a-responsible-media-supply-chain/.

Reporters Without Borders (2020). Official website. https://rsf.org/en.

Reppert-Bismarck, J. (Ed.) (2019). *Tackling disinformation face to face – Journalists' findings from the classroom*. Brussels, Belgium: Lie-detectors. https://lie-detectors.org/wp-content/uploads/2019/09/JournalistsFindings_final.pdf.

Rutenberg, J. (2017, Sept. 13). RT, Sputnik and Russia's new theory of war. *New York Times*. https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html.

Salim, S. (2019, December 31). Facebook claims to regulate its policies – amidst criticism. *Digital Information World*. https://www.digitalinformationworld.com/2019/12/facebook-claims-to-regulate-its-policies-amidst-the-criticism.html.

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. New York, NY: Eamon Dolan Books / Houghton Mifflin Harcourt.

StopFake (2020, Jan. 22). *How "fake news" and disinformation were spread in the run-up to Taiwan's presidential elections*. StopFake blog. https://www.stopfake.org/en/how-fake-news-and-disinformation-were-spread-in-the-run-up-to-taiwan-s-presidential-elections/.

Telegraph (2017, May 24). Qatar state news agency 'hacked with fake positive story about Israel and Iran'. *The Telegraph*. https://www.telegraph.co.uk/news/2017/05/24/qatar-state-news-agency-hacked-fake-positive-story-israel-iran/.

The Computational Propaganda Project (2020). Official website. https://comprop.oii.ox.ac.uk/.

Thompson, N. & Lapowsky, I. (2018, December 17). How Russian trolls used meme warfare to divide America. *Wired*. https://www.wired.com/story/russia-ira-propaganda-senate-report/.

Tsetsura, K. (2020a, November). *Three challenges of mediated construction of soft power as an enabling environment*. Paper to be presented at the NCA convention, Indianapolis, IN.

Tsetsura, K. (2020b, October). *The Matryoshka Effect: Communicating with courage in multi-layered contexts*. Paper to be presented at the World PR Forum, Auckland, New Zealand.

Tsetsura, K., & Kruckeberg, D. (2017). *Transparency, public relations and the mass media: Combating the hidden influences in news coverage worldwide*. New York, NY: Taylor and Francis.

Venturini, T., & Rogers, R. (2019). "API-Based Research", or how can digital sociology and journalism studies learn from the Facebook and Cambridge Analytica data breach. *Digital Journalism*, *7*(4), 532–540. https://doi.org/10.1080/21670811.2019.1591927.

vom Orde, H., & Durner, A. (2019). *Grunddaten Jugend und Medien 2019* [Basic data youth and media 2019] (pp. 105–110). Munich, Germany: Internationales Zentralinstitut fuer das Jugend- und Bildungsfernsehen.

Williams, S. E. (2019, November 13). East Aleppo residents sent text messages from regime giving them 24 hours to leave. *The Telegraph*. https://www.telegraph.co.uk/news/2016/11/13/east-aleppo-residents-sent-text-messages-from-regime-giving-them/.

Wood, D. (2019, September 17). China used Twitter to disrupt Hong Kong protests, but efforts began years earlier. *NPR*. https://www.npr.org/2019/09/17/758146019/china-used-twitter-to-disrupt-hong-kong-protests-but-efforts-began-years-earlier.

Zannettou, S., Caulfield, T., Blackburn, J., De Cristofaro, E., Sirivianos, M., Stringhini, G., & Suarez-Tangil, G. (2018). On the origins of memes by means of fringe web communities. *ACM Internet Measurement Conference*. http://arxiv.org/abs/1805.12512.

Hybrid CoE