# HOW RUSSIA DEFLECTS ACCUSATIONS OF CYBERATTACKS AND DISINFORMATION CAMPAIGNS: AN ANALYSIS OF THE RHETORICAL STRATEGIES OF RT

*Julius Koppel, Sten Hansson*

**ABSTRACT**. The government of the Russian Federation is using cyberattacks and information operations against other countries for geopolitical purposes[1]. Despite being criticised by international communities, Russia deflects all accusations by justifying its behaviour. To better understand the strategic communication of Russia we analysed the ways in which the largest Russian state-funded international news portal RT.com portrays accusations of cyber- and disinformation attacks. According to our analysis, the articles in RT deflect blame from Russia primarily in four ways: (1) accusations are described as groundless and evidence non-existent; (2) accusers are portrayed as malignant and Russia as the victim; (3) accusers are portrayed as unreliable or ridiculous; and (4) the audience is distracted or made to question the accusations.

**Keywords**: Russia, strategic communication, cyberattack, information warfare, blame avoidance, RT

## 1. Introduction

In addition to traditional warfare, the Russian Federation is actively focused on hybrid warfare, using, among other things, different information technology tools and channels of influence for geopolitical purposes[2]. This involves cyberattacks as well as the distribution of malignant, deceitful or false

[1] The article is written as part of research project O-014 "Strategic Narrative as a Model for Reshaping the Security Dilemma" (8 March 2019–31 January 2023).

[2] **Jasper, S**. 2020. Russian Cyber Operations: Coding the Boundaries of Conflict. Washington, D.C.: Georgetown University Press; [**Jasper** 2020] **Lupion, M.** 2018. The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News. – The Journal of Slavic Military Studies, Vol. 31, No. 3.

information in news and social media. Cyberattacks may be used to impair national computer networks, steal delicate information (incl. health data) or disrupt the provision of vital services. For example, a cyberattack on Ukraine in 2015 left a quarter million people without electricity[3]. The purpose of disinformation campaigns may be continuous manipulation of the citizens of other countries, resulting in these citizens supporting the ideas of the manipulator, or disunity amongst them and a loss of trust in democratic institutions.

Characteristically of cyber- and disinformation attacks, it is often impossible to assign blame: the people behind a cyberattack are difficult to identify and false information may be presented in a concealed manner. This gives the accused party the chance to deflect all accusations, using rhetorical strategies for blame avoidance. The ability to identify such strategies makes analysts as well as media consumers more critical of messages distributed by Russian state-funded channels and helps to unveil their potential tools of influence.

This article is focused on the linguistic aspects of how accusations of cyberattacks and disinformation campaigns are deflected in the state-funded Russian media channel RT; the aim is to draw attention to the most common means of blame avoidance in Russian rhetoric. The sample includes 27 English-language articles about accusations against Russia for its cyber- and information attacks published in RT.com in 2018–2020. The most telling examples are discussed in detail in the analysis section. RT is used as an example because it is the largest news network for international audiences financed by the Kremlin. The articles were chosen from the past few years to get an overview of the most recent strategies of blame avoidance. The sample was constructed, first, by searching for articles that included keywords regarding cyberattacks and disinformation and, second, by selecting all articles about accusations or justifications regarding cyber- and disinformation attacks. The background of the analysis is presented with a short overview of cyberattacks and disinformation campaigns in the RT news portal and of linguistic strategies of blame avoidance.

[3] **Xiang, Y.; Wang, L.; Liu, N**. 2017. Coordinated attacks on electric power systems in a cyber-physical environment. – Electric Power Systems Research, Vol. 149.

## 2. Russian cyberattacks and disinformation

Historically, Russia has sought to realise its ambitions of power with deficient resources, resulting in the inevitable use of asymmetrical methods of warfare[4]. These methods that can produce considerable results with relatively small effort include cyberattacks and disinformation campaigns.

A cyberattack is an attack in cyberspace that results, for example, in stealing or modifying data or gaining control over different systems[5]. Cyberattacks enable one to comprehensively impair the functioning of an entire country by causing damage to its state information systems. In 2007, Estonia became the target of Russian cyberattacks[6]. Back then, the attacks did not have a significant impact but Russia had already understood the potential of cyberspace. In order to create such conditions that benefit Russia in cyberspace, the country has taken a leading role in several international summits on cyber and information security since the mid-1990s, enabling Russia to direct these topics in a manner that best suits it[7]. The deficiency of international rules imposed on cyber space benefits Russia because it allows it to harm other countries (for example, intervene in their elections) for its own international interests and purposes without any negative consequences for Russia[8].

Malignant false information or disinformation is knowingly distributed untrue or misleading information aimed at harming something or somebody[9]. Disinformation campaigns and propaganda attacks are known to be part of the arsenal of Russia for affecting local debates of the European Union and neighbouring countries with the purpose of diluting the unity of the European Union and undermining its reputation among neighbouring

[4] **Galeotti, M**. 2016. Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? – Small Wars & Insurgencies, Vol. 27, Issue 2.

[5] **Bruijn, H. de; Janssen, M**. 2017. Building cybersecurity awareness: The need for evidence-based framing strategies. – Government Information Quarterly, Vol. 34, No. 1, p. 1.

[6] **Cohen, R. S.; Radin, A**. 2019. Russia's Hostile Measures in Europe: Understanding the Threat. Santa Monica, California: RAND Corporation. [**Cohen, Radin** 2019]

[7] **Thomas, T**. 2014. Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? – The Journal of Slavic Military Studies, Vol. 27, Issue 1, p. 102.

[8] **Jasper** 2020, p. 3.

[9] **Wardle, C.; Derakhshan, H**. 2017. Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe report DGI(2017)09, p. 5. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (10.06.2020).

countries[10]. According to Russia, information warfare is constantly fought in the entire world and it involves Russia[11]. The current information warfare of Russia is a sequel to the propaganda of the Soviet Union. The general principles of the Cold War era disinformation campaigns have remained almost unchanged, but are now applied online. This includes affecting the media of other countries by offering them entirely or partially falsified stories and by recruiting local journalists as well as using shadow organisations to affect the internal politics of other countries. While the goal has remained the same, the quantity, quality, and measures have changed, which is why contemporary propaganda is more active but harder to identify and control[12]. According to researchers, Western Countries have not succeeded in imposing asymmetric forces equivalent to those of Russian information warfare, for example, forceful sanctions against the members of the Russian State Duma[13]. However, the European Union and NATO have financed and published reports that accuse Russia of cyber- and disinformation attacks and offer potential solutions for countering them[14].

[10] **Meister, S**. (ed.) 2018. Understanding Russian Communication Strategy: Case Studies of Serbia and Estonia. – ifa (Institut für Auslandsbeziehungen) Edition Culture and Foreign Policy. https://www.ssoar.info/ssoar/bitstream/handle/document/59979/ssoar-2018-meister-Understanding_Russian_Communication_Strategy_Case.pdf (26.05.2020). [**Meister** 2018]; **Hellman, M.; Wagnsson, C**. 2017. How can European states respond to Russian information warfare? An analytical framework. – European Security, Vol. 26, Issue 2.

[11] **Mölder, H.; Sazonov, V**. 2018. Information Warfare as the Hobbesian Concept of Modern Times. – The Principles, Techniques, and Tools of Russian Information Operations in the Donbass. – The Journal of Slavic Military Studies, Vol. 31, Issue 3.

[12] **Fedchenko, Y**. 2016. Kremlin propaganda: Soviet active measures by other means. – Sõjateadlane (Estonian Journal of Military Studies), Vol. 2. Tartu: Eesti Ülikoolide Kirjastus; **Rid, T**. 2020. Active Measures: The Secret History of Disinformation and Political Warfare. London: Profile Books.

[13] **Thornton, R**. 2015. The Changing Nature of Modern Warfare. – RUSI Journal, Vol. 160, Issue 4.

[14] See, for example, **Cohen, Radin** 2019. See also **Lucas, E.; Pomerantsev, P**. 2017. Winning the Information War Redux: Techniques and Counterstrategies to Russian Propaganda in Central and Eastern Europe. Extended and Revised Edition. Center for European Policy Analysis (CEPA). https://cepa.ecms.pl/files/?id_plik=4803 (22.07.2020). See also **Sazonov, V.; Müür, K.; Mölder, H**. 2016. Russian Information Campaign Against Ukrainian State and Defence Forces. – NATO Strategic Communications Centre of Excellence, April 26. https://www.ksk.edu.ee/wp-content/uploads/2017/02/Report_infoops_08.02.2017.pdf (23.07.2020).

## 3. Russian state-funded news portal RT

RT (formerly Russia Today) is a global news network (TV, radio, online platforms, etc.) funded by the Russian Federation[15]. According to RT, the size of its weekly audience is 100 million people, whereas the largest proportion of its audience, 43 million followers, are in European countries.

RT is often associated with promoting the interests of Russia; in academic literature, it is referred to as a Russian propaganda channel[16]. At the same time, RT also produces diverse, difficult to confirm and, at times, contradictory content in addition to direct propaganda. Its goal is to sow confusion and doubt to increase its audience's scepticism towards Western journalism, governments, and institutions[17]. RT is trying to undermine the liberal democracy of the West while distributing ideas that benefit the Russian Federation and enforce a positive image of Russia[18]. At the same time, RT claims to defend traditional liberal democratic ideas such as freedom of speech, critical journalism, and independent thinking. Such use of soft power is supported by guest authors from the West whose commentaries are always presented by RT as advocating for the goals of Russia[19].

For these reasons, a report about the strategies of the editorial board of RT compiled by Monika L. Richter, an analyst with the Kremlin Watch Program at the European Values Think-tank, concludes that it is entirely appropriate to call RT an instrument of Kremlin disinformation and a hostile foreign

[15] **RT**. https://www.rt.com/about-us/ (27.04.2020).

[16] **Meister** 2018; **Orttung, R. W.; Nelson, E**. 2018. Russia Today's strategy and effectiveness on YouTube. – Post-Soviet Affairs, Vol. 35, Issue 3; [**Orttung, Nelson** 2018] **Richter, M. L**. 2017. The Kremlin's Platform for 'Useful Idiots' in the West: An Overwiev of RT's Editorial Strategy and Evidence of Impact. – European Values. Kremlin Watch Report. https://www.kremlinwatch.eu/userfiles/the-kremlin-s-platform-for-useful-idiots-in-the-west-an-overview-of-rt-s-editorial-strategy.pdf (04.10.2021). [**Richter** 2017]; **Ventsel, A.; Madisson, M.-L**.; **Hansson, S**. 2021. Russia's Strategic Blame Narratives: Comparative Analysis of Domestic and International Media Coverage About 5G. – Mölder, H.; Sazonov, V.; Chochia, A.; Kerikmäe, T. (eds.). The Russian Federation in Global Knowledge Warfare. Cham: Springer; **Hansson, S.; Madisson, M.-L.; Ventsel, A**. 2022. Discourses of blame in strategic narratives: The case of Russia's 5G stories. – European Security. https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2057188 (15.09.2022). [**Hansson, Madisson, Ventsel** 2022]

[17] **Miazhevich, G**. 2018. Nation branding in the post-broadcast era: The case of RT. – European Journal of Cultural Studies, Vol. 21, Issue 5; **Richter** 2017.

[18] **Orttung, Nelson** 2018, p. 78.

[19] **Richter** 2017, p. 37.

influencer[20]. Ilya Yablokov, a specialist on Russian media at the University of Leeds, describes RT as a Russian tool to undermine the global position of the United States of America by portraying Russia as the main counter-power to the international threat supposedly posed by the USA[21].

The influence of RT largely depends on the extent to which various local media channels and influential public figures share its contents[22]. Claims about the influence of Kremlin disinformation channels should be treated with caution: if one portrayed these as incredibly harmful, it could have the effect of increasing their influence[23].

## 4. Method of analysing rhetorical blame avoidance

In politics, becoming a target of public accusations or scandals may destroy the reputation of a person or organisation and result in the loss of a job or power. This is why politicians, governments, and state officials usually try to either avoid or deflect such accusations[24]. To avoid blame, political actors use a range of linguistic means that include portraying people and activities involved in the blame issue in a suitable manner, and using particular strategies of arguing, legitimising, and denying[25]. Some linguistic and rhetorical devices used for avoiding blame can be considered societally problematic because they can be used to mislead people, prevent a rational public debate on some topics, affect policies and unions, and also justify harmful activities or behaviour[26].

[20] **Richter** 2017, p. 37.

[21] **Yablokov, I**. 2015. Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT). – Politics, Vol. 35, Issue 3/4.

[22] **Richter** 2017, p. 4.

[23] *Ibid*., p. 38.

[24] **Weaver, R. K**. 1986. The Politics of Blame Avoidance. – Journal of Public Policy, Vol. 6, No. 4; **Hood, C**. 2011. The Blame Game: Spin, Bureaucracy, and Self-Preservation in Government. Princeton, NJ: Princeton University Press.

[25] **Hansson, S**. 2015. Discursive strategies of blame avoidance in government: A framework for analysis. – Discourse & Society, Vol. 26, Issue 3. [**Hansson** 2015]

[26] *Ibid*. See also **Hansson, S**. 2018. The discursive micro-politics of blame avoidance: Unpacking the language of government blame games. – Policy Sciences, Vol. 51, Issue 4. [**Hansson** 2018]; **Hansson, S**. 2019. Brexit and blame avoidance: Officeholders' discursive strategies of self-preservation. – Koller, V.; Kopf, S.; Miglbauer, M. (eds.). Discourses of Brexit. London: Routledge.

It is reasonable to presume that the stories published in RT as a Russian state-funded channel are there to deflect different accusations against Russia, including accusations of organising cyberattacks and disinformation campaigns in accordance with the interests of Russia. Based on earlier methodological literature[27], we searched for the following typical linguistic strategies of blame avoidance from the texts of RT that we included in our sample.

1. Deleting verbal references to attackers, potential victims, losses, and suffering. Never mentioning any violations committed by or the negative character traits of an accused party. Avoiding associating a negative deed with the accused party or presenting the deed and the party in the same context.
2. Using linguistic, visual, and other references to magnify the positive aspects of certain incidents or to distract people's attention from the negative. Making bad events or outcomes seem like good ones by using euphemisms (neutralising words or expressions), metaphors (transferring a meaning pursuant to similarities), abstractions, generalisations, and statistics out of context. For example, a cyberattack can be portrayed as an attempt to ascertain the strength of security networks.
3. Reorganising a chain of events to exclude any connections between an act and a negative incident. This will make it seem as if a potentially blameful act was the result of factors independent of the accused party.
4. Legitimising (justifying) problematic activities by referring to authority, shared values, or rational benefits. For example, decisions can be justified via reference to the "recommendations of experts".
5. Portraying oneself as hero or victim and other parties as villains or anti-heroes. For example, the phrase "Another attack against Russia" may make the reader think of Russia as an eternal victim instead of one to be blamed.
6. Denying an offence or its intentionality. Claiming that nothing bad was done, that no bad deed was intentional, or that the person behind the act has been misunderstood. Cyber- and disinformation attacks make it possible to refrain from taking any responsibility because it is often difficult to identify the attacker.

[27] **Hansson** 2015; **Hansson** 2018.

7. Using exaggerated and vague expressions or sowing confusion to modify the perceived nature of deeds and the responsibility of its executers. For example, people who are blamed for cyber and information attacks may use phrases that make people question the existence or reliability of the evidence of these attacks.
8. Emphasising the negative traits of the accuser (*argumentum ad hominem*), their hypocrisy (*tu quoque*), and blaming the victim. For example, attention may be distracted from the content of an accusation by portraying the accuser as malignant or unfair.
9. Providing too much information, offering irrelevant or repetitive information that misleads and distracts people. For example, the accused party can start talking about other accusations or strongly emotional topics to confuse the audience.

Based on these categories, we highlighted relevant sections in our dataset and interpreted them according to the methodology referred to above. Repeated discourse analysis of the dataset revealed that the articles under analysis used four main strategies of blame avoidance. These are discussed in the next chapter.

## 5. Analysis: How does RT deflect accusations of Russia being involved in cyber- and disinformation attacks?

In its articles, the RT news portal deflects accusations against Russia for engaging in cyber- and disinformation attacks primarily in four ways: (1) accusations are described as groundless and evidence non-existent; (2) accusers are portrayed as malignant and Russia as the victim; (3) accusers are portrayed as unreliable or ridiculous; and (4) the audience is distracted or made to question the accusations. We will examine and exemplify these in turn.

### 5.1. Accusations are described as groundless and evidence non-existent

One of the main arguments that RT uses in responding to accusations of Russia having organised cyber and information attacks is the lack of evidence. Even if they admit to an attack having happened, they deny the involvement of Russia. For example, according to *Hacking accusations against Russia a smear campaign timed with NATO cyberwarfare meeting – diplomat*[28], an article commenting on accusations against Russia of cyberattacks and their chronological coincidence with NATO cyberwarfare summits, all accusations are deflected with the inability to prove any blame. RT repeatedly used the phrase *alleged hacking* and claimed that the attacks are without *proper proof*. The phrase *proper proof* may either mean that evidence is lacking or that the existing evidence is improper or untrustworthy. In the article, the ambassador of Russia counters the hacking accusations by claiming that the Western countries

> */…/ used the media to amplify anti-Russian allegations while providing little or no evidence at all to back the claims.*[29]

Insufficient expertise of the USA is mentioned in *'Another propaganda attack': Russian Foreign Ministry hits back over US 'Evil Corp' claims*[30]. The article disapproves of the sanctions established by USA against 11 Russian citizens and six companies whose malware was allegedly involved in cyberattacks, stealing over 100 million dollars from different Western institutions. According to RT, the existing evidence is not adequate to be presented to "specialists":

> *While Washington constantly accuses Russia of "hacking," including the 2016 US presidential election, it refuses to present any proof of those claims, because the US "simply has no evidence that would not be embarrassing to put on the table in front of specialists".*[31]

Even though the specialists mentioned remain unidentified, RT makes it seem as if the USA only employs amateurs and it would be "embarrassing" to present the alleged evidence to real specialists. This supports the claim that no accusations from USA are to be taken seriously.

[28] **Hacking accusations against Russia a smear campaign timed with NATO cyberwarfare meeting – diplomat** 2018. – RT, October 4. https://www.rt.com/news/440344-hacking-allegations-ambassador-interview/ (15.06.2020). [**Hacking accusations against Russia** 2018]

[29] *Ibid.*

[30] **'Another propaganda attack': Russian Foreign Ministry hits back over US 'Evil Corp' claims** 2019. – RT, December 6. https://www.rt.com/news/475234-russian-foreign-ministry-response-us-sanctions-cyber/ (05.06.2020). [**'Another propaganda attack'** 2019]

[31] *Ibid.*

Deflecting the accusations of USA in *Another 'highly likely'-style accusation: Moscow brushes aside 'evidence-free' Georgia cyberattacks*[32], an article about the claims that Russian military intelligence organised a cyberattack against Georgian websites, RT presents the following argumentation:

> *Notably, Russia's accusers were tight-lipped on what evidence they had to support their claims. Neither technical details of the attack nor even a brief explanation of the investigation process were provided. The Russian foreign ministry pointed to this fact as it brushed aside the accusation. "The lack of evidence and political motivation behind this obviously orchestrated information attack are impossible to miss," it said in a statement. "It took almost four months to make an attempt to scapegoat Russia for the incident that happened on October 28 last year. All the charges are along the lines of the notorious 'highly likely' approach," they concluded, referring to the line used by former UK Prime Minister Theresa May when accusing Russia following the poisoning of Sergei Skripal in 2018.*[33]

The first two sentences challenge the existence of evidence because, apparently, the accusers have shared neither the technical details of the attack nor an explanation of the investigation process with Russia. In the third sentence, RT stresses that the Russian Ministry of Foreign Affairs is denying the accusations and quotes the statement given by the Ministry according to which the accusations are only based on the assumption that Russia is "likely" to be blamed without providing any evidence. At the same time the article deflects the accusation of poisoning Skripal, a strategic move referring to a historical chain of accusations against Russia, portraying it as a persecutee. This is examined more thoroughly in the next subchapter.

Similarly to cyberattacks, RT also portrays accusations against Russia for information attacks as groundless. For example, in *Washington fails to provide proof for alleged Moscow-backed Covid-19 disinformation campaign – Russian Foreign Ministry*[34], RT claims that Russian diplomats have been unable to collect any evidence from the USA that would support the accusations that Moscow is leading a disinformation campaign regarding the coronavirus. "Washington fails to provide proof" are the first words of the title and the lack or unsuitability of evidence is referred to throughout the entire article.

[32] **Another 'highly likely'-style accusation: Moscow brushes aside 'evidence-free' Georgia cyberattack** 2020. – RT, February 21. https://www.rt.com/news/481374-russia-georgia-cuber-attack-blame/ (12.05.2020). [**Another 'highly likely'-style accusation** 2020]

[33] *Ibid.*

[34] **Washington fails to provide proof for alleged Moscow-backed Covid-19 disinformation campaign – Russian Foreign Ministry** 2020. – RT, April 9. https://www.rt.com/news/485422-russia-coronavirus-fake-news/ (17.05.2020). [**Washington fails to provide proof** 2020]

> *Russian diplomats called on their US counterparts to provide some actual evidence of allegations circulated by American media and officials that Moscow is waging a coronavirus-themed fake news campaign – but have received none.*[35]

In addition, RT writes that all the allegations are "baseless and without substance", "remain unsupported by evidence", and are "notably lacking facts". Therefore, RT repeats the phrase *groundless accusations* in various forms and justifies this by claiming that Russia has not received any meaningful or factual evidence for any accusations. Furthermore, the article ends with an evaluation by a British researcher who analysed a European External Action Service report and found it to be "groundlessly accusing". RT has cited these two researchers before[36] because their views suit RT well. The objectivity of these sources has been questioned, for example, by Sarah Hurst, a journalist of an independent newspaper Byline Times. She says that the researchers in question are known to draw faulty conclusions by mistranslating Russian and to describe Putin as a pleasant ruler whose actions are justified because NATO is aggressively expanding its Eastern wing[37]. Therefore, to deflect accusations, RT uses seemingly authoritative Western representatives whose opinions will make the audience doubt the truthfulness of Western accusations.

### 5.2. Accusers are portrayed as malignant and Russia as the victim

In order to deflect accusations, RT portrays Russia as a victim who is constantly bullied by others (the Western countries). Such a portrayal is supported by one of the main strategic narratives of Russia, that of a 'Russophobic' attitude of the West, suggesting that Western countries have adopted a negative mindset regarding Russia and the Russian culture[38]. Take, for example, *Hacking accusations against Russia a smear campaign timed with NATO cyberwarfare*

[35] **Washington fails to provide proof** 2020.

[36] **Malic, N**. 2020. No Covid-19 fake news on RT, EU accusations are 'problematic' – UK watchdog. – RT, April 7. https://www.rt.com/news/485230-eu-russian-disinformation-debunked/ (15.04.2020).

[37] **Hurst, S**. 2020. UK Academics Get Hefty Grant to 'Reframe Russia'. – Byline Times, April 14. https://bylinetimes.com/2020/04/14/uk-academics-get-hefty-grant-to-reframe-russia/ (30.04.2020).

[38] **Darczewska, J.; Żochowski, P**. 2015. Russophobia in the Kremlin's Strategy: A Weapon of Mass Destruction. – Point of View, Issue 56. Warsaw: Centre for Eastern Studies (OSW); **Ventsel, A.; Hansson, S.; Madisson, M.-L.; Sazonov, V**. 2018. Hirmu mehhanismid strateegilistes narratiivides õppuse Zapad 2017 näitel. – Sõjateadlane, No. 8. [Cultural, Peace and Conflict Studies Series, Vol. VIII]. Tartu: Eesti Ülikoolide Kirjastus. [**Ventsel *et al.*** 2018]

*meeting – diplomat*[39], an article about how a NATO cyberwarfare summit is connected with accusing Russia. The first sentence of the article constructs a general understanding about Russia being constantly under attack since the word latest refers to a number of previous attacks: "*The latest wave of accusations against Russia.*"[40]

The notion of a *wave* refers to a flow of several continual accusations. This determines the opposing parties—Russia versus all others—along with the definite victim position of Russia. This could refer to bullying where it is common for a group to offend an individual, and not the other way around. This view is supported by expressions such as "coordinated media attack" which also refers to the existence of more than one attacker. While the article initially mentions single Western countries, the reasoning of the Russian diplomat cited in the article expands the notion of *bullies* to all Western countries: "*Yakovenko added that there was a pattern of behaviour by Western nations /…/*".[41]

An article about condemning the USA sanctions, *'Another propaganda attack': Russian Foreign Ministry hits back over US 'Evil Corp' claims*, also differentiates between the "good guys" and the "bad guys"[42]. It is constantly emphasised in the article that Russia is looking to maintain good relations and cooperate, but that the USA is not interested. In a way, it portrays the USA as a villain that is constantly throwing around groundless accusations and is unwilling to find a solution together. Russia's attempt to make itself seem as the initiatory party may serve its purpose to come off as the "good guy" who is, unfortunately, forced to deal with false accusations and sanctions.

There are a number of examples of how RT portrays Russia as a typical victim that is constantly attacked in *Another 'highly likely'-style accusation: Moscow brushes aside 'evidence-free' Georgia cyberattack*[43], an article that deflects the blame for cyberattacks against Georgia away from Russia. For instance:

> *Many in Georgia immediately blamed the attack on Russia, and lo and behold, more than three months later the accusation is official.*[44]

[39] **Hacking accusations against Russia** 2018.

[40] *Ibid.*

[41] *Ibid.*

[42] **'Another propaganda attack'** 2019.

[43] **Another 'highly likely'-style accusation** 2020.

[44] *Ibid.*

This section makes Russia seem like a typical victim. The ironic expression "lo and behold" gives the impression of no wonder that Russia is always being blamed. It makes the reader think that this is always the case, a constantly recurring pattern. Regarding the accusations by the USA, the United Kingdom, Canada, and others, the article uses expressions such as "the partners soon piled on Russia," and "make an attempt to scapegoat Russia," confirming the fact that Russia is being portrayed as the victim.

Another reference to Russia being a typical victim that is always blamed for everything can be found in the following section:

> *In the absence of actual proof, people with a record of accusing Russia of various nefarious cyber deeds resorted to speculation. Georgia is "in their neighbourhood," said Adam Meyers from the security firm CrowdStrike. "It's in line with Russian tactics. The specific outcome is less important than causing upheaval and conflict between different groups in the country."*[45]

RT is trying to create the impression that Russia is always blamed by the same people who should not even be listened to because they are pathological speculators without any evidence. The blame avoidance tactic of RT, portraying Russia as the victim, is supported by the 'Russophobia' narrative, also visible in this example. On the one hand, RT confirms the victim status of Russia by portraying Russia as being constantly attacked by certain people, but on the other hand, RT fires a counterattack with *argumentum ad hominem*, making it seem like the accusers of Russia are deeply troubled.

The same article uses another tactic of blame avoidance: switching the positions of the accused and the accuser.

> *The lack of evidence and political motivation behind this obviously orchestrated information attack are impossible to miss /…/.*[46]

Here, RT is portraying the accusers of Russia, i.e., the Western countries, as the ones to blame. According to the Russian Ministry of Foreign Affairs, it is a politically motivated information attack against Russia. Using the word *obviously* is a linguistic means of impact used to avoid providing proof to support one's own claims. Russia is, again, portrayed as a victim under constant attack; the word *orchestrated* refers to several attackers whose actions are coordinated.

The same tactics are used to deflect the accusations of disinformation campaigns regarding the coronavirus in *Washington fails to provide proof for*

[45] **Another 'highly likely'-style accusation** 2020.

[46] *Ibid.*

*alleged Moscow-backed Covid-19 disinformation campaign – Russian Foreign Ministry*[47]. After summarising the accusations against Russia, the media representative of the Russian Ministry of Foreign Affairs cited in the article, Maria Zakharova, reverses the roles of the accuser and the accused party.

> *Several US news outlets have run stories on an alleged fear-mongering campaign waged by pro-Kremlin media and fearsome social media bots, no less. In addition, conspiracy theories that the coronavirus might have been artificially created by the Russians circulated on social media – and the effort appeared to be coordinated by US government agencies, Zakharova stated. All the accusations remain unsupported by evidence, even after persistent attempts by Russian diplomats to try and get some actual proof of the alleged evil-doing.*[48]

First, the article claims that USA news outlets are accusing Russia of fear-mongering campaigns (first sentence). Then, additional information is introduced that suddenly changes the roles (second sentence), saying that not only is the USA accusing but also attacking Russia by spreading conspiracy theories on social media. Ventsel et al. [49] have said that antithetical logic is a specific blame avoidance method of Russia[50]. Essentially, this means blaming others for the exact same things attributed to oneself. The second sentence of the last cited section perfectly illustrates this strategy.

Ironically, the Russian Ministry of Foreign Affairs does not provide any evidence in accusing the USA for attacks against Russia other than the speculative formation, "appeared to be coordinated by US government agencies."

The position of victim is confirmed in this article by appealing to people's better nature. Russia is portrayed as a moral party and the USA as immoral.

> *The whole course of the coronavirus pandemic has been accompanied by allegations against Russia and – alternately – China and Iran of spreading lies and fear in the West. As if the deadly disease, which has already affected over 1.5 million people globally and killed more than 90,000, was not scary enough as it is.*[51]

[47] **Washington fails to provide proof** 2020.

[48] *Ibid.*

[49] **Ventsel, A.; Hansson, S.; Madisson, M.-L.; Sazonov, V**. 2021. Discourse of fear in strategic narratives: The case of Russia's Zapad war games. – Media, War & Conflict, Vol. 14, Issue 1. https://journals.sagepub.com/doi/full/10.1177/1750635219856552 (06.08.2021). [**Ventsel *et al*.** 2021]

[50] See also **Madisson, M.-L.; Ventsel, A**. 2020. Strategic Conspiracy Narratives: A Semiotic Approach. London: Routledge; **Hansson, Madisson, Ventsel** 2022.

[51] **Washington fails to provide proof** 2020.

Here, RT uses an interesting construction: the fact that COVID-19 was a terrible global disease seems to rule out the possibility of Russia spreading fear and lies in the West. It might create a (faulty) impression as if the pandemic forced Russia to stop all geopolitical influence activities for an unspecified period of time. In this way, RT appeals to the emotions of the audience, presenting tragic statistics that makes accusing Russia seem disgraceful.

A seamless switch of the roles of the accuser and the accused supports the constant victim position of Russia. For example, there is a sentence in the same article that portrays Russia as an eternal scapegoat, and suggests that blaming Russia will guarantee success for the accusers in the West: "*The fail-proof 'blame Russia' approach persisting in the West in recent years /…/*"[52].

Such a portrayal is, again, supported by the 'Russophobia' narrative. RT portrays Russia as the victim in the same article also in a section about a report by the European External Action Service that reveals Russia's disinformation. According to RT, this report was "*composed almost entirely of 'scary Russians' tropes /…/*[53]*.*"

### 5.3. Accusers are portrayed as unreliable or ridiculous

RT often portrays the representatives of Western countries that accuse Russia of cyber and information attacks as unreliable or ridiculous, trying to undermine the credibility of the accusations against Russia.

Take, for example, *We want to believe: 'Russian hacking' memo REVEALS how US intel pinned leaks to Kremlin*[54], an article commenting on documents about the potential interference of Russia in the American presidential elections of 2016 that had been disclosed on the previous day. The author of this article, Nebojsa Malic, ridicules the creators of the document and claims that all accusations against Russia are based on the *belief* held by a narrow group of people that Russia is guilty.

> *Reading through it, one is struck by the circular reasoning of the US "intelligence community" – or rather, Clapper's hand-picked group of CIA, FBI and NSA people charged with coming up with the assessment. The US intelligence*

[52] **Washington fails to provide proof** 2020.

[53] *Ibid.*

[54] **Malic, N**. 2018. We want to believe: 'Russian hacking' memo REVEALS how US intel pinned leaks to Kremlin. – RT, November 10. https://www.rt.com/usa/443644-russia-hacking-methods-election-memo/ (08.06.2020). [**Malik** 2018]

> *community is "confident" that the Russian government was behind the "compromises" of emails, because their release is "**consistent with the methods and motivations** of Russian-directed efforts," the talking points say. In other words, this fits what US spies believe are Russian objectives, therefore it had to be the Kremlin doing it!*[55]

The recurring topic of the article is related with an alleged *circular reasoning*, an error in the logical argumentation of US intelligence agencies, mentioned in the first sentence of the cited section and more thoroughly explained in the second and third sentence of the same section: all USA's accusations against Russia are solely based on the *belief* of the American intelligence people that Russia is guilty. Therefore, if American officials consider an activity to be characteristic of Russia then Russia is probably to blame. The author of the article equates this logic with an unproven "belief", making the creators of the report seem incredible.

Malic also questions the involvement of the authors of the report in the USA intelligence community, using "intelligence community" in quotation marks and reasoning that they are rather a group of people selected by James Clapper, director of national intelligence (first sentence). Even though the article lists three large US organisations known for their involvement in intelligence, the quotation marks seem to suggest that the people of these organisations are not part of the intelligence community. This also challenges the credibility of the report. In later discussions about the intelligence community, quotation marks are no longer used, but at the beginning of the second sentence, the word "confident" is in quotation marks. Here, Malic acknowledges the existence of the intelligence community but ridicules the conclusions of their report and, therefore, the entire intelligence community of USA. As for the conclusions based on beliefs, according to Malic, the intelligence community cannot, therefore, be convinced that Russia is behind a variety of activities. In the final sentence of the cited section, the authors of the report are called 'spies', a word possibly carrying a negative connotation in this context. A similar belittling manner is used in *Washington fails to provide proof for alleged Moscow-backed Covid-19 disinformation campaign – Russian Foreign Ministry*[56], an article about the accusations of spreading false information regarding the coronavirus, calling the strategic communication department of the European External Action Service a propaganda branch.

[55] **Malik** 2018.

[56] **Washington fails to provide proof** 2020.

The credibility of the USA's representatives is also questioned in *Russia isn't only behind election hacking! They're also trying to smear US over coronavirus … according to State Department*[57], an article deflecting the accusations of spreading disinformation regarding the coronavirus. Discussing the accusations, the article claims that the institution behind these is untrustworthy, and no evidence has been presented. An accusation by a US envoy, the director of the Global Engagement Centre (GEC), regarding the negative impact that Russia has on US-China relations is followed by undermining the capability of the GEC. For example, RT suggests that it is unclear whether the GEC has collected any information on the potential Russian disinformation campaign regarding the coronavirus by using the phrase "supposedly gathered in a report." The article emphasises that the activities of the Global Engagement Centre have been doubtful before. According to RT, the Centre was accused of belittling the people who criticised the Iran-related policy of President Trump. Any such reference to the (alleged) negative traits or (alleged) past malpractice of an accuser helps to undermine the credibility of an accuser and their accusations.

### 5.4. Confusing the audience

In addition to the argumentations to deflect blame, RT has also been known to mislead the reader in order to distract their attention from accusations or confuse them.

For example, *Another 'highly likely'-style accusation: Moscow brushes aside 'evidence-free' Georgia cyberattack*[58], an article about cyberattacks against Georgia, uses a recurring stealth narrative to demonise or mystify Russian cyber power. Its purpose may be to distract the attention of readers away from the accusations by Georgia, the USA, Canada, and other countries, according to which the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) is responsible for the cyberattacks against Georgia. The article begins with the claim that, allegedly, over 15,000 websites were a

[57] **Russia isn't only behind election hacking! They're also trying to smear US over coronavirus … according to State Department** 2020. – RT, February 22. https://www.rt.com/usa/481485-coronavirus-russia-state-department/ (05.05.2020). [**Russia isn't only behind election hacking!** 2020]

[58] **Another 'highly likely'-style accusation** 2020.

target of the attack, whereas according to BBC News[59], the number was much more modest, amounting to over 2,000. Inflating the numbers may benefit Russia. First, it helps to create the impression that the information regarding the accusations is controversial and, therefore, the accusations might not have a solid ground. Second, the higher the number of websites that were allegedly attacked, the higher seem to be the abilities of the attacker. This may turn the focus of the audience away from the accusations against Russia towards the scale and complexity of the attack. Displaying power by manipulating numbers has been previously analysed by Ventsel et al.[60] in publications on Russian fear-narratives.

Notably, the same RT article also mentions the US presidential elections of 2016 in which Russia allegedly intervened, and the poisoning of Skripal the double agent in 2018[61]. A discussion about events that have lost relevance helps to distract the reader from the accusations of cyberattacks against Russia. A rhetorical association between different historic attacks also helps to portray Russia as a powerful and dangerous international actor. Referring to the allegedly extensive influence and cyber power of GRU may make the readers perceive Russia as a superpower. Confusion, mystery, and room for speculation are also added by the final sentence of the article which refers to Russian companies that, according to RT, suffered from malware attacks whose extent was comparable to that of an armed cyberattack and that originated from the USA's national intelligence agency: "*Among their victims were Russian oil giant Rosneft, metal-maker Evraz and the Russian Central Bank.*"[62]

An unexpected inclusion of previous events is also detected in *Russia isn't only behind election hacking! They're also trying to smear US over coronavirus … according to State Department*[63], an article about disinformation regarding the coronavirus. The title alone claims that not only has Russia intervened in elections but is now also trying to disparage the USA in relation to the coronavirus. A false accusation is associated with a cyberattack incident from four years ago, probably making the reader wonder about the presidential elections in the USA and any potential interference by Russia. This helps to distract people's attention away from a specific incident while also suggesting

[59] **UK says Russia's GRU behind massive Georgia cyber-attack** 2020. – BBC, February 20. https://www.bbc.com/news/technology-51576445 (23.05.2020).

[60] **Ventsel *et al.*** 2018, pp. 103–127; **Ventsel *et al.*** 2021.

[61] **Another 'highly likely'-style accusation** 2020.

[62] *Ibid.*

[63] **Russia isn't only behind election hacking!** 2020.

that Russia is internationally incredibly powerful. In the same article, RT reconfirms the impression of an extensive operation, describing in detail all the alleged activities for which Russia is blamed. For example, according to the article, thousands of real people, and not mere bots, were involved in the campaign, every single one of them having gotten the green light from the Russian government to undermine the reputation of the USA. The article recites the claims that even the media channels RT and Sputnik were accused of being involved in the campaign. This all makes the reader think of the extent of the attack, diverts the focus of the article away from specific accusations, and emphasises the international grasp and power of Russian activities.

For the purpose of magnifying mystery and confusing the reader even further, the final section of the article ridicules the idea that Russia is blamed for intervening in the presidential elections of the USA:

> *For those keeping track at home, US officials have now blamed Russia for not only using the coronavirus to try and hurt the US' "reputation," but they have also conspired with Trump to win the 2016 election /…/.*[64]

As explained by Ventsel et al.[65], such a ridiculing tone might add mystery and, thus, amplify the image of Russia as a superpower. This, in turn, might distract the attention of readers away from the accusations against Russia for spreading disinformation.

## 6. Conclusion

Russia uses state-funded media channels to justify its policies and actions as well as to deflect blame from Russia. This analysis revealed that there are four main ways in which Russia deflects accusations of cyber- and disinformation attacks in the stories published in its RT news portal.

First, Russia claims that the accusations against it are groundless because they are not based on solid facts confirmed by Russian experts. RT quotes the public statements of the Russian government, denying any blame for cyber- and disinformation attacks, and uses quotes by Western spokespeople in a manner that enables doubt to be sown on the truthfulness of the accusations.

Second, in stories about cyberattacks and disinformation campaigns, RT portrays Russia as the victim and the accusers of Russia—mainly the USA—

[64] **Russia isn't only behind election hacking!** 2020.

[65] **Ventsel *et al.*** 2021.

as villains. This is done with words and expressions that indicate that Russia is the one always being blamed by the Western countries while Russia just wishes to repair its relations with them. Constructing a victim position like that is based on the historic narrative of 'Russophobia'.

Third, to portray the accusers of Russia as unreliable and to ridicule them, RT describes them in an undermining manner using evaluative words with negative connotations, questioning their knowledge. In order to avoid taking the blame, RT says that the accusations against Russia are often merely based on the "belief" of the USA or the Western countries that Russia is guilty.

Fourth, RT tries to confuse the audience by directing their attention away from accusations or distracting them. To do that, RT associates accusations against Russia with other (historic) events and portrays Russia as a superpower.

Readers should adopt a critical attitude towards all content published by RT because the stories that RT presents as news are written in accordance with Russia's foreign policy goals. The stories portray the member states of NATO as incompetent and divided, and evoke distrust against Western democratic institutions. Russia is concurrently portrayed both as a victim and as an international superpower. Persistent denial of the use of cyberattacks and disinformation campaigns seems to be a convenient strategy for Russia: it is difficult for the member states of NATO and the European Union to launch a counterattack against Russia's cyberattacks or establish sanctions in response to its disinformation campaigns because there are often no legal grounds for it. The impact of cyber- and disinformation attacks, however, may be devastating for other countries and threaten their sovereignty. This is why the communicative self-defence tactics adopted by Russia definitely deserve closer inspection. For example, the researchers of RT and other similar propaganda channels should reveal Russia's blame avoidance strategies regarding its human rights violations, and also analyse the strategic uses of images, not just texts, in security-related blame games.

## Bibliography

**Another 'highly likely'-style accusation: Moscow brushes aside 'evidence-free' Georgia cyberattack** 2020. – RT, February 21.
https://www.rt.com/news/481374-russia-georgia-cuberattack-blame/ (12.05.2020).

**'Another propaganda attack': Russian Foreign Ministry hits back over US 'Evil Corp' claims** 2019. – RT, December 6.
https://www.rt.com/news/475234-russian-foreign-ministry-response-us-sanctions-cyber/ (05.06.2020).

**Bruijn, H. de; Janssen, M**. 2017. Building cybersecurity awareness: The need for evidence-based framing strategies. – Government Information Quarterly, Vol. 34, No. 1, p. 1.

**Cohen, R. S.; Radin, A**. 2019. Russia's Hostile Measures in Europe: Understanding the Threat. Santa Monica, California: RAND Corporation.

**Darczewska, J.; Żochowski, P**. 2015. Russophobia in the Kremlin's Strategy: A Weapon of Mass Destruction. – Point of View, Issue 56. Warsaw: Centre for Eastern Studies (OSW).

**Fedchenko, Y**. 2016. Kremlin propaganda: Soviet active measures by other means. – Sõjateadlane (Estonian Journal of Military Studies), Vol. 2. Tartu: Eesti Ülikoolide Kirjastus, pp. 141–170.

**Galeotti, M**. 2016. Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? – Small Wars & Insurgencies, Vol. 27, Issue 2, pp. 282–301.

**Hacking accusations against Russia a smear campaign timed with NATO cyberwarfare meeting – diplomat** 2018. – RT, October 4.
https://www.rt.com/news/440344-hacking-allegations-ambassador-interview/ (15.06.2020).

**Hansson, S**. 2015. Discursive strategies of blame avoidance in government: A framework for analysis. – Discourse & Society, Vol. 26, Issue 3, pp. 297–322.

**Hansson, S**. 2018. The discursive micro-politics of blame avoidance: Unpacking the language of government blame games. – Policy Sciences, Vol. 51, Issue 4, pp. 545–564.

**Hansson, S**. 2019. Brexit and blame avoidance: Officeholders' discursive strategies of self-preservation. – Koller, V.; Kopf, S.; Miglbauer, M. (eds.). Discourses of Brexit. London: Routledge.

**Hansson, S.; Madisson, M.-L.; Ventsel, A**. 2022. Discourses of blame in strategic narratives: The case of Russia's 5G stories. – European Security. https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2057188 (15.09.2022).

**Hellman, M.; Wagnsson, C**. 2017. How can European states respond to Russian information warfare? An analytical framework. – European Security, Vol. 26, Issue 2, pp. 153–170.

**Hood, C**. 2011. The Blame Game: Spin, Bureaucracy, and Self-Preservation in Government. Princeton, NJ: Princeton University Press.

**Hurst, S**. 2020. UK Academics Get Hefty Grant to 'Reframe Russia'. – Byline Times, April 14.
https://bylinetimes.com/2020/04/14/uk-academics-get-hefty-grant-to-reframe-russia/ (30.04.2020).

**Jasper, S**. 2020. Russian Cyber Operations: Coding the Boundaries of Conflict. Washington, D.C.: Georgetown University Press.

**Lucas, E.; Pomerantsev, P**. 2017. Winning the Information War Redux: Techniques and Counterstrategies to Russian Propaganda in Central and Eastern Europe. Extended and Revised Edition. Center for European Policy Analysis (CEPA).
https://cepa.ecms.pl/files/?id_plik=4803 (22.07.2020).

**Lupion, M**. 2018. The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News. – The Journal of Slavic Military Studies, Vol. 31, No. 3, pp. 329–353.

**Madisson, M.-L.; Ventsel, A**. 2020. Strategic Conspiracy Narratives: A Semiotic Approach. London: Routledge.

**Malic, N**. 2018. We want to believe: 'Russian hacking' memo REVEALS how US intel pinned leaks to Kremlin. – RT, November 10.
https://www.rt.com/usa/443644-russia-hacking-methods-election-memo/ (08.06.2020).

**Malic, N**. 2020. No Covid-19 fake news on RT, EU accusations are 'problematic' – UK watchdog. – RT, April 7. https://www.rt.com/news/485230-eu-russian-disinformation-debunked/ (15.04.2020).

**Meister, S**. (ed.) 2018. Understanding Russian Communication Strategy: Case Studies of Serbia and Estonia. – ifa (Institut für Auslandsbeziehungen) Edition Culture and Foreign Policy.
https://www.ssoar.info/ssoar/bitstream/handle/document/59979/ssoar-2018-meister-Understanding_Russian_Communication_Strategy_Case.pdf (26.05.2020).

**Miazhevich, G**. 2018. Nation branding in the post-broadcast era: The case of RT. – European journal of Cultural Studies, Vol. 21, Issue 5, pp. 575–593.

**Mölder, H.; Sazonov, V**. 2018. Information Warfare as the Hobbesian Concept of Modern Times. – The Principles, Techniques, and Tools of Russian Information Operations in the Donbass. – The Journal of Slavic Military Studies, Vol. 31, Issue 3, pp. 308–328.

**Orttung, R. W.; Nelson, E**. 2018. Russia Today's strategy and effectiveness on YouTube. – Post-Soviet Affairs, Vol. 35, Issue 3, pp. 1–16.

**Richter, M. L.** 2017. The Kremlin's Platform for 'Useful Idiots' in the West: An Overwiev of RT's Editorial Strategy and Evidence of Impact. – European Values. Kremlin Watch Report.
https://www.kremlinwatch.eu/userfiles/the-kremlin-s-platform-for-useful-idiots-in-the-west-an-overview-of-rt-s-editorial-strategy.pdf (04.10.2021).

**Rid, T**. 2020. Active Measures: The Secret History of Disinformation and Political Warfare. London: Profile Books.

**RT**. https://www.rt.com/about-us/ (27.04.2020).

**Russia isn't only behind election hacking! They're also trying to smear US over coronavirus … according to State Department** 2020. – RT, February 22.
https://www.rt.com/usa/481485-coronavirus-russia-state-department/ (05.05.2020).

**Sazonov, V.; Müür, K.; Mölder, H**. 2016. Russian Information Campaign Against Ukrainian State and Defence Forces. – NATO Strategic Communications Centre of Excellence, April 26.
https://www.ksk.edu.ee/wp-content/uploads/2017/02/Report_infoops_08.02.2017.pdf (23.07.2020).

**Thomas, T**. 2014. Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? – The Journal of Slavic Military Studies, Vol. 27, Issue 1, pp. 101–130.

**Thornton, R**. 2015. The Changing Nature of Modern Warfare. – RUSI Journal, Vol. 160, Issue 4.

**UK says Russia's GRU behind massive Georgia cyber-attack** 2020. – BBC, February 20. https://www.bbc.com/news/technology-51576445 (23.05.2020).

**Ventsel, A.; Hansson, S.; Madisson, M.-L.; Sazonov, V**. 2018. Hirmu mehhanismid strateegilistes narratiivides õppuse Zapad 2017 näitel. – Sõjateadlane, No. 8. Cultural, Peace and Conflict Studies Series, Vol. VIII. Tartu: Eesti Ülikoolide Kirjastus.

**Ventsel, A.; Hansson, S.; Madisson, M.-L.; Sazonov, V**. 2021. Discourse of fear in strategic narratives: The case of Russia's Zapad war games. – Media, War & Conflict, Vol. 14, Issue 1.
https://journals.sagepub.com/doi/full/10.1177/1750635219856552 (06.08.2021)

**Ventsel, A.; Madisson, M.-L.; Hansson, S**. 2021. Russia's Strategic Blame Narratives: Comparative Analysis of Domestic and International Media Coverage About 5G. – Mölder, H.; Sazonov, V.; Chochia, A.; Kerikmäe, T. (eds.). The Russian Federation in Global Knowledge Warfare. Cham: Springer.

**Wardle, C.; Derakhshan, H**. 2017. Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe report DGI(2017)09, p. 1–109.
https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (10.06.2020).

**Washington fails to provide proof for alleged Moscow-backed Covid-19 disinformation campaign – Russian Foreign Ministry** 2020. – RT, April 9.
https://www.rt.com/news/485422-russia-coronavirus-fake-news/ (17.05.2020).

**Weaver, R. K**. 1986. The Politics of Blame Avoidance. – Journal of Public Policy, Vol. 6, No. 4.

**Xiang, Y.; Wang, L.; Liu, N**. 2017. Coordinated attacks on electric power systems in a cyber-physical environment. – Electric Power Systems Research, Vol. 149.

**Yablokov, I**. 2015. Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT). – Politics, Vol. 35, Issue ¾.

Second Lieutenant (res.) **JULIUS KOPPEL**, MA
Public relations adviser at Ministry of Rural Affairs of Estonia

**STEN HANSSON**, PhD
Associate professor of Communication at the Institute of Social Studies, University of Tartu, and Marie-Skłodowska-Curie research fellow at the University of Birmingham (the United Kingdom)