Securitization of Disinformation in NATO's Lexicon: A Computational Text Analysis

Akın Ünver
Özyeğin University

Ahmet Kurnaz
Çanakkale Onsekiz Mart University

Abstract

Following the Russian meddling in the 2016 US elections, disinformation and fake news became popular terms to help generate domestic awareness against foreign information operations globally. Today, a large number of politicians, diplomats, and civil society leaders identify disinformation and fake news as primary problems in both domestic and foreign policy contexts. But how do security institutions define disinformation and fake news in foreign and security policies, and how do their securitization strategies change over years? Using computational methods, this article explores 238,452 tweets from official NATO and affiliated accounts, as well as more than 2,000 NATO texts, news statements, and publications since January 2014, presenting an unsupervised structural topic model (stm) analysis to investigate the main thematic and discursive contexts of these texts. The study finds that NATO's threat discourse and securitization strategies are heavily influenced by the US' political lexicon, and that the organization's word choice changes based on their likelihood of mobilizing alliance resources and cohesion. In addition, the study suggests that the recent disinformation agenda is, in fact, a continuity of NATO's long-standing Russia-focused securitization strategy and their attempt to mobilize the Baltic states and Poland in support of NATO's mission.

Keywords: Securitization, NATO, Russia, text analysis, structural topic model

1. Introduction

In recent years, disinformation, information warfare, and fake news have become important strategic and political concepts in international relations.[1] Although these terms are just as old as the term 'propaganda', their mainstream use in the context of digital communication skyrocketed after the 2016 US elections.[2] Even before the elections, these terms had begun to enter the foreign policy discourse of the North Atlantic Treaty Organization (NATO) countries

Akın Ünver, Associate Professor, Department of International Relations, Özyeğin University. Email: akin.unver@ozyegin.edu.tr. 0000-0002-6932-8325.

Ahmet Kurnaz, Research Assitant, Political Science and Public Administration, Çanakkale Onsekiz Mart University. Email: ahmetkurnaz@hotmail.com. 0000-0001-5628-328X.

[1] Alexander Lanoszka, "Disinformation in International Politics," *European Journal of International Security* 4, no. 2 (June 2019): 227–48, https://doi.org/10.1017/eis.2019.6; Christina la Cour, "Theorising Digital Disinformation in International Relations," *International Politics* 57, no. 4 (2020): 704–23.

[2] Nir Grinber g et al., "Fake News on Twitter during the 2016 U.S. Presidential Election," *Science* 363, no. 6425 (2019): 374–78.

Received: 04.05.2021 Accepted:31.01.2022

following the 2014 Russian military operations in Ukraine. Prior to the annexation of Crimea, Russia had already designated information warfare as part of its 2010 Military Doctrine, which was updated again in 2014 with a special emphasis on digital communication.[3] A year prior to that, the importance of the digital space for military doctrinal considerations was outlined by General Valery Gerasimov, the Russian Chief of the General Staff. In his 2013 article titled 'The Value of Science is in the Foresight', Gerasimov wrote: "*The very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. … All this is supplemented by military means of a concealed character.*"[4] These three statements are generally accepted as the doctrinal basis of modern Russian information operations that were demonstrated in Ukraine in 2014, and also later in Syria in late 2015.[5]

Since then, strategic communicative actions that are intended to influence, mislead, and confuse foreign populations have assumed a central position in global debates about politics and foreign policy. Given the impact of such actions on elections, polarization, and crisis management, it was natural for the rhetoric about these actions to assume such a central position.[6] However, over time, popular buzzwords like 'disinformation/misinformation', 'fake news', and 'information operations' have proliferated in global political mainstream discourse, assuming an accusatory nature worldwide as more leaders, diplomats, and politicians have begun using them to discredit and delegitimize their political opponents. This dynamic was later conceptualized as 'discursive deflection'[7] and has become acutely visible in the foreign policy domain as more countries have begun securitizing the concepts 'fake news', 'disinformation', and 'information warfare' to similarly discredit and delegitimize rival countries.[8] Broadly speaking, 'discursive-deflection' is the strategy of discrediting competitors and rivals by portraying oneself as the sole source of truth. While the domestic political use of these terms is well-studied, we are still somewhat in the dark with regard to why countries choose to securitize these terms and what happens in their interactions with other countries when they do so.

The foreign policy use of such terms predates the 2016 US elections and proliferated after the Russian military involvement in Crimea and Donbas.[9] The primary reason for this contextual proliferation was the Russian decision to deny the initial stages of both its involvement in Ukraine and its broader strategy of distracting and dividing Western attention over Russian military operations.[10] There is still a debate over whether it was really Russian information operations that had derailed NATO's response in Ukraine, or if disinformation

[3] Bettina Renz, "Russian Military Capabilities after 20 Years of Reform," *Survival* 56, no. 3 (2014): 61–84.

[4] Mark Galeotti, "The Mythical 'Gerasimov Doctrine' and the Language of Threat," *Critical Studies on Security* 7, no. 2 (2019): 157–61.

[5] Polina Sinovets and Bettina Renz, "Russia's 2014 Military Doctrine and beyond: Threat Perceptions, Capabilities and Ambitions," NATO Research Papers (Rome: NATO Defense College, July 2015), https://www.ndc.nato.int/news/news.php?icode=830.

[6] Samantha Bradshaw and Philip N. Howard, "The Global Organization of Social Media Disinformation Campaigns," *Journal of International Affairs* 71, no. 1.5 (2018): 23–32.

[7] Andrew S. Ross and Damian J. Rivers, "Discursive Deflection: Accusation of 'Fake News' and the Spread of Mis- and Disinformation in the Tweets of President Trump," *Social Media + Society* 4, no. 2 (2018), doi: https://doi.org/10.1177/2056305118776010; Christopher A Smith, "Weaponized Iconoclasm in Internet Memes Featuring the Expression 'Fake News,'" *Discourse & Communication* 13, no. 3 (2019): 303–19.

[8] Matthew A. Baum and Philip B. K. Potter, "Media, Public Opinion, and Foreign Policy in the Age of Social Media," *The Journal of Politics* 81, no. 2 (2019): 747–56.

[9] Irina Khaldarova and Mervi Pantti, "Fake News," *Journalism Practice* 10, no. 7 (2016): 891–901.

[10] Ulises A Mejias and Nikolai E Vokuev, "Disinformation and the Media: The Case of Russia and Ukraine," *Media, Culture & Society* 39, no. 7 (2017): 1027–42.

discourses are employed in order to shift the blame over to Russia for the time when NATO was already divided over its commitment to Ukraine.[11] While there is robust evidence of Russian information operations in Ukraine and their role in spreading disinformation in NATO countries, NATO's sustained apathy towards the rising Russian military influence in the Black Sea after 2014 and in Syria after 2015 support the latter claim.

Critics of Western disinformation discourses, for example, argue that such discourses have turned into 'floating (or empty) signifiers' that have no specific or agreed-upon meaning.[12] In that vein, blaming others for engaging in disinformation often detracts attention from a mistake or failed policy enacted by the blamer.[13] In this case, critics argue that Western discourses on disinformation are intended to distract attention from NATO or EU divisions, or more domestic-level polarization dynamics, by creating a unique empty signifier (disinformation) to be employed as a rallying rhetoric that bolsters the significance of external threats.[14] In this way, disinformation and its associated terms, like misinformation, fake news, and information war, get securitized, receiving disproportionate levels of attention in the policy domain. In this context, disinformation and its associated terms are used to exaggerate an existing threat and create a rallying discourse meant to channel the attention of divided Western nations away from their internal disagreements and towards an inflated external threat. Some scholars go even further, arguing that disinformation is being securitized in the West (especially in NATO) to the extent that the 'war on terror' was securitized through the 2000s.[15] In this line, disinformation is alleged to have become a new strategic glue intended to help Western nations pool together their increasingly diverging interests and resources in support of a common cause.[16]

Securitization of disinformation in domestic politics is relatively well-studied.[17] Although these terms entered mainstream debates after the 2016 US elections, former President Donald Trump, too, securitized fake news to delegitimize his opponents by constructing rival disinformation as a national security problem, indirectly attributable to China.[18] Following the tornado of accusations in the US, political actors in Britain, France, Italy, South Africa, Kenya and others have begun blaming each other for engaging in organized disinformation.[19] Even in Sweden, there is empirical evidence that suggests accusing journalists of spreading fake news results in the self-censorship of such outlets.[20] There are further cases of evidence

[11] Volodymyr Lysenko and Catherine Brooks, "Russian Information Troops, Disinformation, and Democracy," *First Monday* 23, no. 5 (2018), doi: https://doi.org/10.5210/fm.v22i5.8176.

[12] Johan Farkas and Jannick Schou, "Fake News as a Floating Signifier: Hegemony, Antagonism and the Politics of Falsehood," *Javnost - The Public* 25, no. 3 (2018): 298–314.

[13] Linda Monsees, "'A War against Truth' - Understanding the Fake News Controversy," *Critical Studies on Security* 8, no. 2 (2020): 116–29.

[14] Lluís Mas-Manchón et al., "Patriotic Journalism in Fake News Warfare: El País' Coverage of the Catalan Process," *The Political Economy of Communication* 8, no. 2 (2021), http://www.polecom.org/index.php/polecom/article/view/123.

[15] Lanoszka, "Disinformation in International Politics."

[16] Mario Baumann, "'Propaganda Fights' and 'Disinformation Campaigns': The Discourse on Information Warfare in Russia-West Relations," *Contemporary Politics* 26, no. 3 (2020): 288–307.

[17] Deen Freelon and Chris Wells, "Disinformation as Political Communication," *Political Communication* 37, no. 2 (2020): 145–56. Ric Neo, "When Would a State Crack Down on Fake News? Explaining Variation in the Governance of Fake News in Asia-Pacific," *Political Studies Review* (2021), doi: https://doi.org/10.1177%2F14789299211013984.

[18] Francesca Polletta and Jessica Callahan, "Deep Stories, Nostalgia Narratives, and Fake News: Storytelling in the Trump Era," in *Politics of Meaning/Meaning of Politics: Cultural Sociology of the 2016 U.S. Presidential Election*, ed. Jason L. Mast and Jeffrey C. Alexander, Cultural Sociology (Cham: Springer International Publishing, 2019), 55–73.

[19] Florian Saurwein and Charlotte Spencer-Smith, "Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe," *Digital Journalism* 8, no. 6 (2020): 820–41; Jacinta Mwende Maweu, "'Fake Elections'? Cyber Propaganda, Disinformation and the 2017 General Elections in Kenya," *African Journalism Studies* 40, no. 4 (2019): 62–76.

[20] W. Lance Bennett and Steven Livingston, "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions," *European Journal of Communication* 33, no. 2 (2018): 122–39.

supporting the claim that elite-level discourses on disinformation have a direct effect on how society perceives information and facts in general, creating a measurable effect on public trust towards such facts and information.[21] In Singapore, for example, delegitimizing rival parties and news outlets through disinformation discourse is considered 'acceptable' as part of the state's duty to discipline the opposition and its political actors.[22] Similar trends emerging in democracies and authoritarian countries alike, such as in Austria, Australia, Poland, Russia, and South Africa, demonstrate the universality of instrumentalizing disinformation discourse as a political delegitimization tactic.[23]

While a robust scholarship is emerging on the domestic political uses of disinformation discourse, there has so far been no longitudinal large-N study that explores how such constructions emerge in international politics. Furthermore, there has yet to be an exploration of how such discourses evolve over time, and under what contexts, in foreign affairs. We know that disinformation and fake news are important issues in world politics and that they are frequently used to bring an issue to public attention, but we remain in the dark over the contextual and temporal nuances that drive the ways in which these concepts are discursively constructed in foreign policy discourse.

This study aims to provide an early addition to the emerging literature on foreign policy uses of disinformation discourses by focusing on how the NATO has used them in its documents and social media posts. It does so by studying 238,452 tweets from official NATO and affiliated accounts, as well as more than 2,000 NATO texts, news statements, and publications since January 2014, and by using computational methods to present an unsupervised structural topic model (stm) analysis that explores the main thematic and discursive contexts of these texts. Ultimately, we hope to trigger a wider debate on the securitization of disinformation and fake news in foreign policy, and also to shed light on the greater explanatory value of computational methods in studying large-N text data based on such securitization strategies.

2. Securitizing Disinformation

Over the last few years, defining misleading content and measuring the legitimacy of its dissemination have been at the forefront of journalistic, political, and scientific debates.[24] Even before its proliferation in 2016, disinformation was a widely-used term in mainstream discourse, co-existing with other terms such as infoglut, or information overload.[25] While disinformation and misinformation were first used interchangeably, today, disinformation refers to the deliberate dissemination of false information with the intention of misleading and confusing an audience. Misinformation, on the other hand, strictly refers to the unintended diffusion of false information without malintent. There are also bridge terms such as 'malinformation', which refers to information that is factually accurate but is deployed to damage the image of an individual or an entity, or the concept of 'problematic information' as

[21] Emily Van Duyn and Jessica Collier, "Priming and Fake News: The Effects of Elite Discourse on Evaluations of News Media," *Mass Communication and Society* 22, no. 1 (2019): 29–48.

[22] Netina Tan, "Electoral Management of Digital Campaigns and Disinformation in East and Southeast Asia," *Election Law Journal: Rules, Politics, and Policy* 19, no. 2 (2020): 214–39.

[23] Edson C. Tandoc Jr, Zheng Wei Lim, and Richard Ling, "Defining 'Fake News,'" *Digital Journalism* 6, no. 2 (2018): 137–53. Xymena Kurowska, and Anatoly Reshetnikov, "Neutrollization: Industrialized Trolling as a Pro-Kremlin Strategy of Desecuritization," *Security Dialogue* 49, no. 5 (2018): 345-63.

[24] Jr, Lim, and Ling, "Defining 'Fake News'".

[25] Mark Andrejevic, *Infoglut: How Too Much Information Is Changing the Way We Think and Know* (New York: Routledge, 2013).

defined by Caroline Jack.[26] Although it is not directly mentioned, all of these concepts refer to the digital space, where information manipulation is disseminated faster and more broadly on social media and digital communication technologies as compared to other forms of media.

As the terms 'disinformation/misinformation', 'fake news', 'information operation', and 'hybrid war' are often used interchangeably in political discourse, there are little clear-cut differences in the strategic meaning of each word choice.[27] Politicians and leaders often use these terms as a bag of buzzwords without a clear operational definition of what each term precisely means. All of these buzzwords generate roughly the same effect, the delegitimization of their target, on consumers of such messages.[28] Especially problematic is the fact that once the discourse on disinformation is weaponized to delegitimize rivals, there is very little such rivals can do to defend themselves. Given the significant political charge of these terms, individuals or institutions that are alleged to be engaging in disinformation-related activities often have to enter into a fruitless spar of words to challenge such allegations, which usually leads to further controversy. This renders the accuser – or the side that securitizes disinformation – more advantageous compared to the accused, generating a dynamic similar to the 'attacker's advantage' in cyber security, where the defender is continuously blindsided.[29]

Therefore, the securitization of disinformation – that is, discursively constructing disinformation as a security concern – is becoming almost as controversial as disinformation itself, and can often be deployed to muddle the waters of a healthy debate. Its problem lies within its success; namely, how successfully disinformation gets securitized and rallies policy resources around itself. This fits into Buzan et. al.'s criteria for a 'successful speech-act', which should take place in a medium most appropriate for its dissemination and have a clear, mobilizable referent object (i.e. 'those that spread disinformation').[30] By securitizing disinformation in the medium that is most conducive for its dissemination (social media and the Internet), speakers get a chance to use the speed and volume advantage of digital communication technologies against their opponents. Also, such discursive constructions must be sedimented (1) rhetorically: have a clear argumentative function, (2) discursively: contain clear power and hegemonic relations within, (3) culturally: refer to a well-known case or instance, and (4) institutionally: in a way that mobilizes policy resources.[31]

Yet, for the Copenhagen school, not all speech acts constitute securitization. Securitization is a very particular discursive construct that designates a specific existential threat requiring the mobilization of uncommon resources and measures that go beyond the norms of institutional and political responses.[32] In many cases, securitization happens to trigger and

[26] Susan Morgan, "Fake News, Disinformation, Manipulation and Online Tactics to Undermine Democracy," *Journal of Cyber Policy* 3, no. 1 (2018): 39–43; Caroline Jack, "Lexicon of lies: Terms for Problematic Information," *Data & Society* 3, no. 22 (2017): 1094-096.

[27] Andrew M. Guess and Benjamin A. Lyons, "Misinformation, Disinformation, and Online Propaganda," in *Social Media and Democracy: The State of the Field, Prospects for Reform*, ed. Joshua A. Tucker and Nathaniel Persily, SSRC Anxieties of Democracy (Cambridge: Cambridge University Press, 2020), 10–33.

[28] Joshua A. Tucker et al., "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature," *Hewlett Foundation* (blog), March 19, 2018, https://hewlett.org/library/social-media-political-polarization-political-disinformation-review-scientific-literature/.

[29] Chau Tong et al., "'Fake News Is Anything They Say!' — Conceptualization and Weaponization of Fake News among the American Public," *Mass Communication and Society* 23, no. 5 (2020): 755–78,.

[30] Barry Buzan, Ole Wæver, and Jaap De Wilde, *Security: A New Framework for Analysis*, UK ed. edition (Boulder, CO: Lynne Rienner Publishers, 1998).

[31] Michael C. Williams, "Words, Images, Enemies: Securitization and International Politics," *International Studies Quarterly* 47, no. 4 (2003): 511–31.

[32] Olav F. Knudsen, "Post-Copenhagen Security Studies: Desecuritizing Securitization," *Security Dialogue* 32, no. 3 (2001): 355–68.

facilitate these institutional changes by 'shocking' power brokers and bureaucracies into action, either through internal bureaucratic peer pressure, or through public opinion pressure (audience costs). As such, disinformation has been lifted 'above politics' in Western rhetoric as a peculiar threat that requires the sidelining of daily political squabbles, mobilizing unique resources, and addressing it in unity that would otherwise not materialize.[33] Ultimately, the discursive constructions of disinformation constitute acute cases of securitization as they generate amity-enmity relations only among countries that adopt this discursive strategy.[34]

Social media offers a unique challenge for the study of securitization. Traditionally, securitizing statements are extracted from lengthy speeches and texts through discourse analysis. However, the advent of faster and higher-volume digital communication technologies have led to a shift of state and elite discourses from older to newer media systems.[35] To that end, due to their word limits, platforms such as Facebook, Twitter, and Instagram do not provide contiguous discursive framing opportunities for researchers to study securitization dynamics.[36] Furthermore, since elite and state-level discourses on social media are often written by assistants, communication representatives, or PR firms, they don't constitute the 'performative actions' that are the cornerstone of securitization.[37] This generates a significant 'context gap' in which researchers may not fully understand the wider thematic and lexical ecosystem that such social media posts may inhabit. Interpreting securitization in such media platforms thus necessitates more robust techniques of 'horizon scanning' that would allow researchers to extract long-term discursive variances and contexts.

Computational text analysis methods largely deliver this horizon scanning. What social media posts lack due to word and character limits, they provide in an immense volume of data that yields ample context in longitudinal analyses. By extracting large quantities of text data from social media, researchers can not only interpret the changing contours and contexts of securitization, but they can also cross-check these findings with more traditional forms of discursive construction outlets such as speeches, documents, and archival material. That is why in this study, we not only engage in a large-scale longitudinal 'old form' securitization analysis by focusing on NATO archives, we also add in 'new form' analysis by extracting a large tweet dataset from official NATO accounts.

The logic of interpreting how disinformation gets securitized by relying on NATO documents is two-fold: first, NATO has been evolving to find new *raisons d'être* since the end of the Cold War and has sought to capitalize on the securitization of new threats, such as terrorism, cybersecurity, Syria, and forced migration.[38] Disinformation and information war are two of the recent additions to this threat portfolio that helps us understand how NATO's discourses on security adapt to a new-medium threat. Second, it enables us to understand how institutional security arrangements like NATO reinvent their security identities and construct their amity-enmity relations in light of newer technologies. Since identity and action are

[33] Barry Buzan and Ole Wæver, "Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory," *Review of International Studies* 35, no. 2 (2009): 253–76.

[34] Buzan and Wæver, "Macrosecuritisation and Security Constellations".

[35] Thierry Balzacq, Sarah Léonard, and Jan Ruzicka, "'Securitization' Revisited: Theory and Cases," *International Relations* 30, no. 4 (2016): 494–531.

[36] Gwen Bouvier and David Machin, "Critical Discourse Analysis and the Challenges and Opportunities of Social Media," *Review of Communication* 18, no. 3 (2018): 178–92.

[37] Carlo Lipizzi et al., "Towards Computational Discourse Analysis: A Methodology for Mining Twitter Backchanneling Conversations," *Computers in Human Behavior* 64 (2016): 782–92.

[38] Holger Stritzel and Sean C. Chang, "Securitization and Counter-Securitization in Afghanistan," *Security Dialogue* 46, no. 6 (2015): 548–67.

considered closely linked in constructivism, and because they are never fixed or intrinsic, but are rather fluid and constituted through social processes, studying longitudinal securitization dynamics gives us valuable insight into long-term NATO security planning.[39]

3. Methodology

Since this study concerns the longitudinal dynamics of how disinformation and related terms were securitized, and since the volume of text that we are dealing with is quite large, we follow a computational methodology that combines social media text data extraction methods with traditional text analysis tools. In recent years, social media data has grown into a useful study area for social scientists as more and more governmental documents become digitized and as governments start taking an active role in social media.[40] While traditional forms of text analysis and discourse analysis approaches use hand coding schemes, newer methods in text mining and analysis are increasingly more preferred due to their ability to process large quantities of text data and eliminate the inter-coder reliability issues from the equation.[41] Moreover, these newer methods increase the causal robustness of text data by building inter- and intra-text causal inferences, strengthening the explanatory power of words as dependent or independent variables.

Table 1 - Descriptive statistics of the text dataset

##	type	all	disinfo	disinfo_ratio	rest
## 1:	tweet	238452	4112	1.72	234340
## 2:	speeches	1136	223	19.63	913
## 3:	press_releases	1083	12	1.11	1071
## 4:	thematic_topics	142	11	7.75	131
## 5:	reviews	119	44	36.97	75
## 6:	official_texts	19	4	21.05	15
## 7:	archives	16	0	0.00	16
## 8:	publications	12	9	75.00	3
## 9:	basic_texts	10	4	40.00	6

Note: 'All' denotes the aggregate number of contents within that specific document type. 'Disinfo' denotes the number of documents that contain disinformation-related keywords within. 'disinfo_ratio' denotes the proportion of documents that contain disinformation-related keywords within the broader pool of documents analyzed.

In order to explore how NATO has securitized disinformation in recent years, we isolated 238,452 tweets from NATO and official affiliated accounts from January 2014 to February 2021 and extracted more than 2000 speeches, press releases, reviews, official texts, archival documents, and publications from the NATO e-library.[42] Out of this sample, we extracted documents and content that contained the keywords 'disinformation', 'misinformation', 'fake news', 'propaganda', 'hybrid warfare' and 'information warfare', and logged the number of their occurrences within these texts by date. Since this study doesn't focus

[39] Maria Mälksoo, "Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO," *European Security* 27, no. 3 (2018): 374–92.

[40] Paul DiMaggio, "Adapting Computational Text Analysis to Social Science (and Vice Versa)," *Big Data & Society* 2, no. 2 (2015), doi: https://doi.org/10.1177/2053951715602908.

[41] Klaus Krippendorff, "Measuring the Reliability of Qualitative Text Analysis Data," *Quality and Quantity* 38, no. 6 (2004): 787–800.

[42] NATO E-Library, https://www.nato.int/cps/en/natohq/publications.htm.

on the semantic differences between these keywords and considers them to be different references to disinformation as a discursive strategy, we code and merge them singularly as the variable '*disinfo*'. Our preliminary analysis shows that NATO has used these keywords most frequently in tweets, followed by speeches, reviews, and publications. However, when analyzed proportionally, NATO publications focus on disinformation most frequently (75% of all documents), followed by tweets (40%), reviews (36.97%), and official texts (21.05%).

Table 2 - The number of occurrences for disinformation-related keywords in each document type

##	type	N
## 1:	speeches	351
## 2:	reviews	63
## 3:	press_releases	14
## 4:	basic_texts	6
## 5:	thematic_topics	15
## 6:	official_texts	6
## 7:	publications	17
## 8:	tweet	4302

In this study, we employ structural topic modeling (STM), a text analysis approach that finds 'topics' in an unstructured corpus based on covariate information.[43] It follows a statistical logic that measures the co-occurrence likelihoods of keywords and terms that are likely to appear with each other, deriving topical meanings out of those likelihoods. Topic modeling is increasingly being used in social sciences for studies of large volumes of text, such as archival documents or social media text datasets, by producing "*each word on the basis of some number of preceding words or word classes,*" and "*generate[ing] words based on latent topic variables inferred from word correlations independent of the order in which the words appear.*"[44] In recent years, topic modeling has become a widely-used method to study large Twitter datasets and political discussions that happen on other social media platforms.[45]

[43] Margaret E. Roberts, Brandon M. Stewart, and Dustin Tingley, "Stm: An R Package for Structural Topic Models," *Journal of Statistical Software* 91, no. 1 (2019): 1–40.

[44] Hanna M. Wallach, "Topic Modeling: Beyond Bag-of-Words," in *Proceedings of the 23rd International Conference on Machine Learning*, ICML '06 (New York, NY, USA: Association for Computing Machinery, 2006), 977–84.

[45] Liangjie Hong and Brian D. Davison, "Empirical Study of Topic Modeling in Twitter," in *Proceedings of the First Workshop on Social Media Analytics*, SOMA '10 (New York, NY, USA: Association for Computing Machinery, 2010), 80–88; Jim Giles, "Computational Social Science: Making the Links," *Nature News* 488, no. 7412 (2012): 448; Hai Liang and King-wa Fu, "Testing Propositions Derived from Twitter Studies: Generalization and Replication in Computational Social Science," *PLOS ONE* 10, no. 8 (2015), doi: https://doi.org/10.1371/journal.pone.0134270.2010

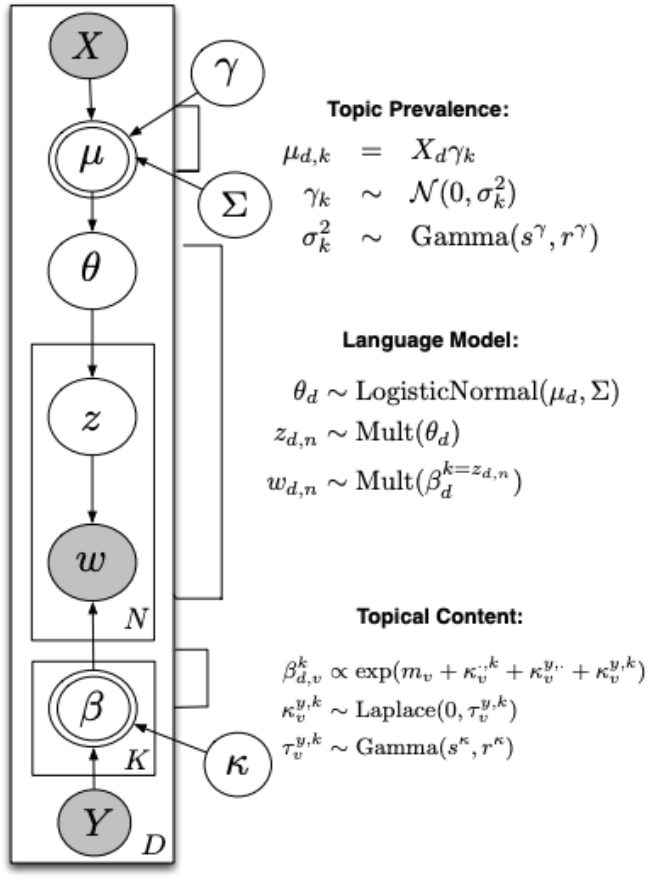

Figure 1: Plate Diagram for Structural Topic Model: "*The model combines and extends three existing models: the correlated topic model (CTM), the Dirichlet-Multinomial Regression (DMR) topic model and the Sparse Additive Generative (SAGE) topic model. The logistic normal prior on topical prevalence in the standard CTM is replaced by a logistic-normal linear model. The design matrix for the covariates X allows for arbitrarily flexible functional forms of the original covariates using radial basis functions (our R package also provides B-splines). The distribution over words is replaced with a multinomial logit such that a token's distribution is the combination of three effects (topic, covariates, topic-covariate interaction) operationalized as sparse deviations from a baseline word frequency (m). Our software provides the analyst with a choice of regularizing priors for the GLM coefficients (κ, γ) with defaults: Normal-Gamma prior pooled by topic for γ and the "Gamma Lasso" prior [10] for κ.*"[46]

[46] Margaret E. Roberts et al., "The Structural Topic Model and Applied Social Science," in *ICONIP2013* (International Conference on Neural Information Processing, Daegu, South Korea, 2013), https://scholar.princeton.edu/files/bstewart/files/stmnips2013.pdf.

A longitudinal analysis of the specific keywords sorted by document type reveals a clear difference in word choice between different NATO documents. In NATO Basic Texts, the most-preferred reference keyword is ‘hybrid warfare’, whereas in press releases, reliance on the word ‘misinformation’ gradually evolves into ‘disinformation’ by 2018. NATO reviews also largely prefer ‘misinformation’, but NATO speeches and tweets are more diverse, with a heavier use of the terms ‘propaganda’, ‘disinformation’, and ‘fake news’. This difference is an interesting demonstration of how elastic these terms are and how different institutional cultures and outlets can prefer one over the other in their communication strategies.

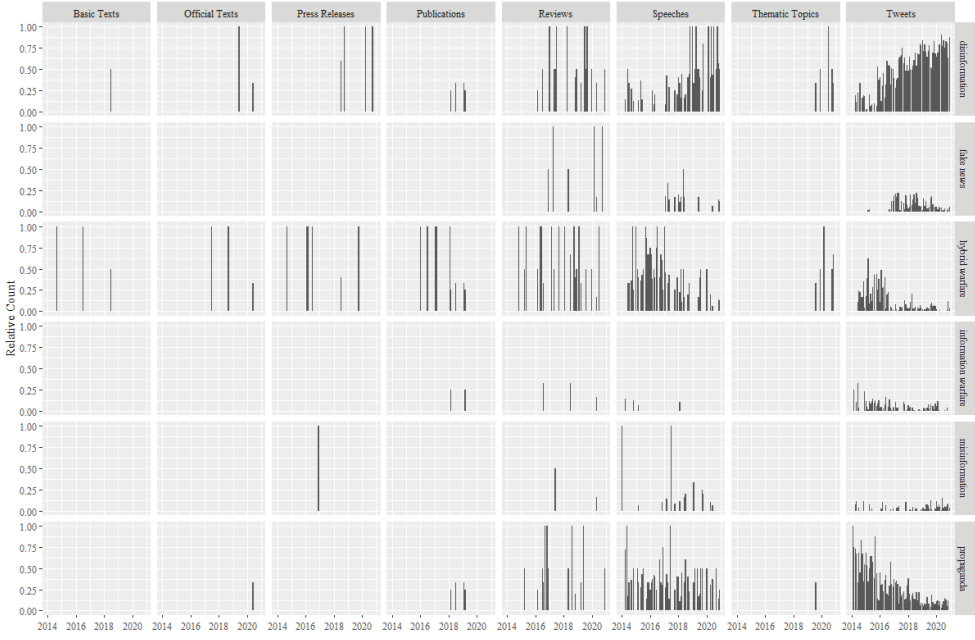

Figure 2: Longitudinal temporal histogram of top keywords (disinformation, fake news, hybrid warfare, information warfare, misinformation, propaganda) as they appear in NATO texts

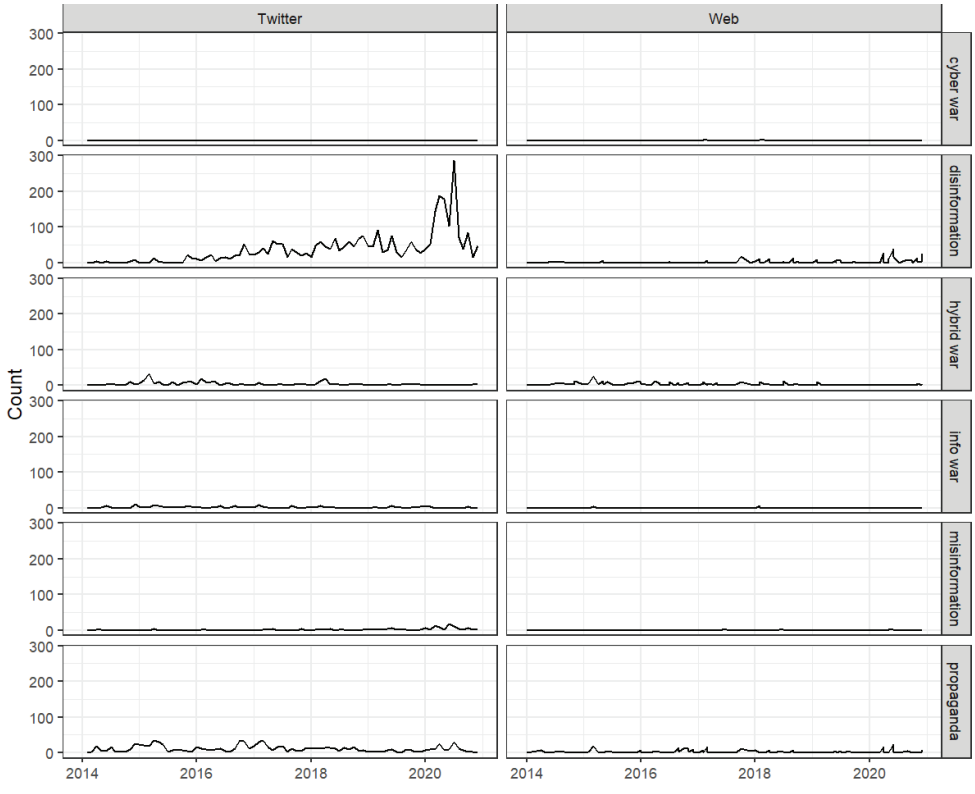

Figure 3: Longitudinal temporal frequency of top keywords as they appear in NATO Twitter texts vs official documents

The differences between NATO official texts and tweets are particularly interesting. Although NATO official texts shift from a 'hybrid war'-focused discourse to 'disinformation'-focused discourse by 2018, the reliance on 'disinformation' discourse in tweets is more striking. By late 2016 (the US elections), 'disinformation' becomes a clear discursive choice in NATO tweets, skyrocketing in much of 2020 due to COVID and vaccine-related securitization discourses globally. This could be interpreted as the discursive anchoring capacity of the United States for NATO, as the constructions of securitization in American political culture affects the wider institutional discourse of NATO. Perhaps as the clearest sign of the temporal variations in word choice shifts, NATO's Twitter accounts use the words 'disinformation', 'information warfare', and 'misinformation' overwhelmingly more often in comparison with its official texts and statements, which rely more on 'cyber war' and 'hybrid war'. As for NATO and affiliated accounts that use the keyword 'disinformation', four clear accounts stand out. These are @STRATCOMCOE (NATO Strategic Communications Centre of Excellence), @NATOmoscow (NATO Information Office Moscow), @NATOBrazeB (NATO Assistant Secretary General for Public Diplomacy), and @NATOpress (Official Twitter account of the @NATO Spokesperson). As for which NATO country representations use this word the most, Latvia (@LV_NATO), Lithuania (@LitdelNATO), United States (@USNATO), Ukraine (@NATOinUkraine) and Germany (@GermanyNATO) stand out the

most.

Table 3- Official NATO-affiliated accounts sorted by the ratio of disinformation-related tweets as part of their aggregate tweets

##	screen_name	V1	ratio
## 1:	STRATCOMCOE	500	19.01
## 2:	NATOmoscow	417	15.86
## 3:	NATOBrazeB	398	15.13
## 4:	NATOpress	231	8.78
## 5:	LV_NATO	119	4.52
## 6:	LitdelNATO	104	3.95
## 7:	NATORomeroC	90	3.42
## 8:	NATO	89	3.38
## 9:	USNATO	82	3.12
## 10:	NATOinUkraine	74	2.81
## 11:	GermanyNATO	62	2.36
## 12:	CanadaNATO	52	1.98
## 13:	ItalyatNATO	45	1.71
## 14:	PLinNATO	43	1.63
## 15:	UKNATO	42	1.60
## 16:	SwedenNato	35	1.33
## 17:	Slovakia_NATO	31	1.18
## 18:	NATODepSpox	27	1.03
## 19:	SHAPE_NATO	23	0.87
## 20:	SpainNATO	23	0.87

Our 'keyness measures'[47] (two-by-two frequencies of words within a sample) indicate that while NATO's official documents are more general with regard to its strategic word choices, NATO's tweets are overwhelmingly focused on the terms 'disinformation', 'propaganda', and 'fake news' within the context of Russia ('pro-Kremlin', 'Russian', and 'Kremlin' designations).

[47] Anna Marchi and Charlotte Taylor, eds., *Corpus Approaches to Discourse: A Critical Review*, 1st edition (New York: Routledge, 2018).

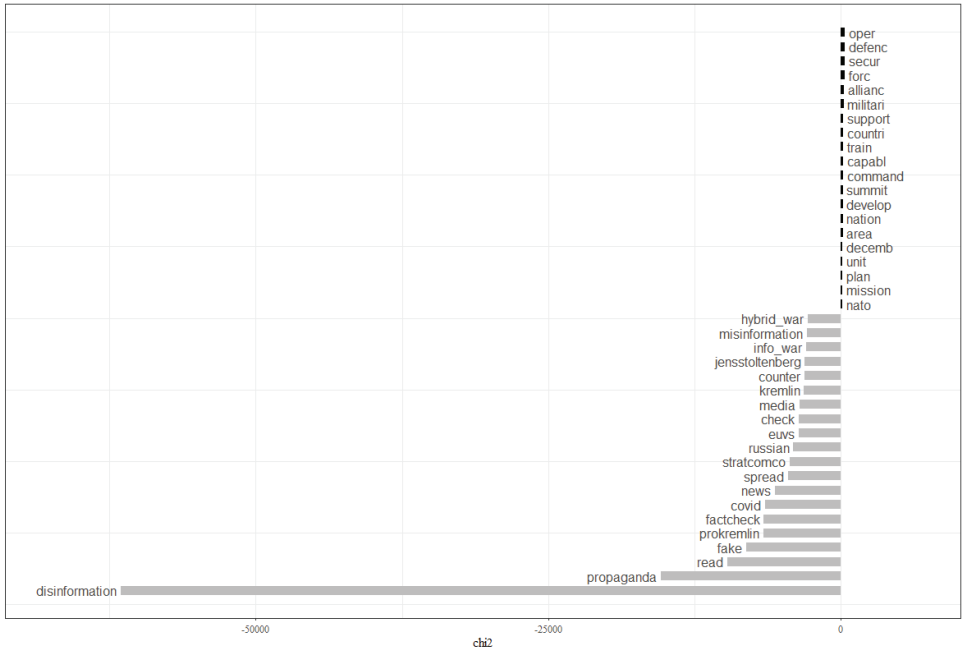

Figure 4: Keyness (textual context – most and least likely correlations) graph of tweets and official documents relative to keyword 'disinformation'. Highest likelihood keyword is itself: 'disinformation'. After that, the plot shows ranked keywords from bottom to up, according to how frequently they appear with the main keyword 'disinformation'.

4. Unsupervised Structural Topic Model Results

For the structural topic models, we used the stm package for R, developed by Molly Roberts, Brandon Stewart and Dustin Tingley.[48] Stm was developed as part of its developers' quest to come up with a methodological tool that would allow them to generate causal inferences from text data. By measuring document-level covariate measures, it introduces a new form of qualitative inference and within-text estimation algorithms for better topic correlations. This ultimately helps us generate more accurate topic associations and themes within complex, lengthy documents.

[48] Roberts, Stewart, and Tingley, "Stm."

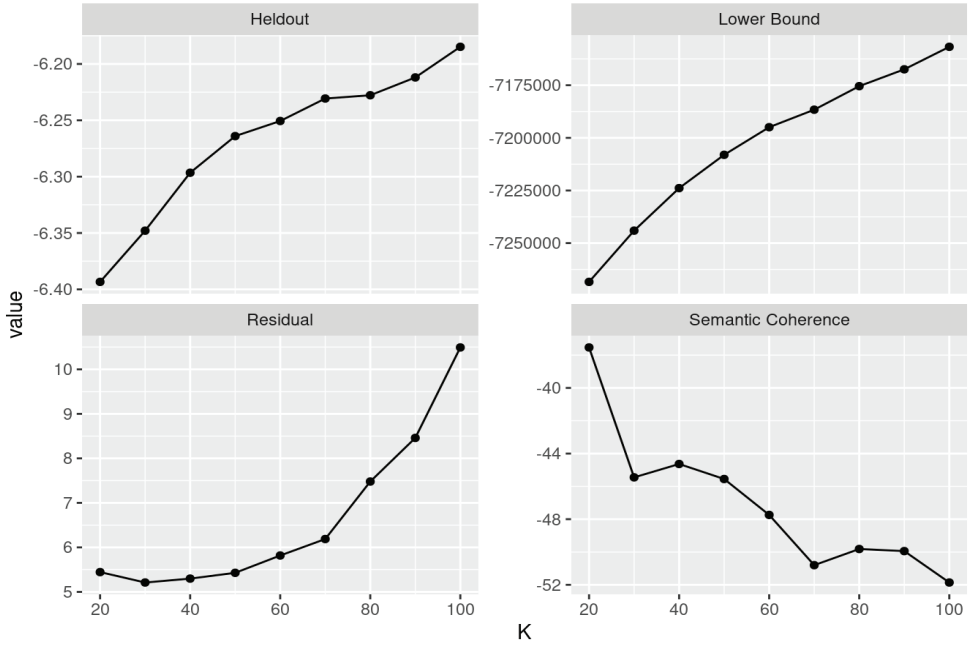

Figure 5: Topic count graph demonstrating the optimization rationale for our stm algorithm's choice of 50 topic models. The 'K-value' shows the optimum number of 'structural topic models' the algorithm has to go through the text to find the optimum semantic coherence. In other words, the K number designates the optimum number of structural topic models in texts that have the highest statistical coherence coefficients. Often, K values are assigned by the programmer and an optimum number gets eyeballed after several trial and error runs. K-value optimization uses machine learning to iterate through the text multiple times to find the optimum K-value by statistical clustering of frequently collocated word combinations.

Our unsupervised machine learning tests within NATO documents and tweets containing disinformation-related trigger words yielded 50 topic models with an optimum combination of semantic coherence and heldout values. Out of these 50 models, our algorithm found that 10 of them had greater semantic salience, and thus had a statistically higher likelihood of forming a coherent 'topic'. Since not all word combination likelihoods imply a theme, K-means clustering is required to measure the co-occurrence likelihood of words that make up a topic in relation to the statistical significance of other topics.[49] These are the topics classified and numbered by our stm algorithm as 1, 4, 7, 9, 14, 16, 23, 35, 39, 47.

Topic 1 demonstrates the over-reliance on the term 'disinformation' as the dominant discursive anchor for NATO documents, mostly correlating with keywords associated with its spread, the role of fact-checking, and misinformation, which is a less-used term. Topic 16 demonstrates that the term 'Russian' is highly correlated with the terms 'fake' and 'news' within the context of info(rmation)_war(fare), as well as 'troll'. The second most salient

[49] Wang, Hongning, Duo Zhang, and ChengXiang Zhai, "Structural Topic Model for Latent Topical Structure Analysis," (Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies, 2011), 1526–535; Margaret E. Roberts, Brandon M. Stewart, Dustin Tingley, Christopher Lucas, Jetson Leder -Luis, Shana Kushner Gadarian, Bethany Albertson, and David G. Rand, "Structural Topic Models for Open- Ended Survey Responses," *American Journal of Political Science* 58, no. 4 (2014): 1064–082.

model is Topic 23, which builds around the keyword 'propaganda'. This model correlates most significantly with the n-gram clusterings: 'strateg_', 'fact', 'truth', and 'counter', suggesting that such emphasis is generally made within the context of combating external propaganda efforts. The third most salient Topic Model is 4, which is built around Russia and the n-grams 'Ukrain_', 'hybrid_war', 'Putin', and 'Moscow'. At least within the context of Russian military involvement in Crimea and Donbass, NATO has largely relied on the term 'hybrid warfare' instead of 'disinformation' or 'misinformation', suggesting that it doesn't consider this military entanglement within the context of 'disinformation'.

To understand NATO's most active institution dealing with disinformation defense, Topic 35 is instructive. There, the keyword 'disinformation' correlates with STRATCOMCOE (NATO Strategic Communications Centre of Excellence in Riga, Latvia) and RigaStratCom, revealing NATO's frontier defense mechanism of choice in issues related to disinformation. This is in line with Topic 30, where geographies correlated with our 'disinformation' keyword cluster reveals 'europ_', 'baltic', 'german_', 'danger', and 'prepar_', hinting at NATO's perceived geographic vulnerability against disinformation attempts. A secondary vulnerability cluster emerges in Topic 49, where the 'lithuania', 'estonia', 'japan', 'poland', and 'baltic' designations correlate with 'target' and 'defens_' n-grams[50]. In Topic 14, we discover the emergence of COVID-related disinformation issues, although the correlated terms are not yet sufficient to infer a political trend of preference.

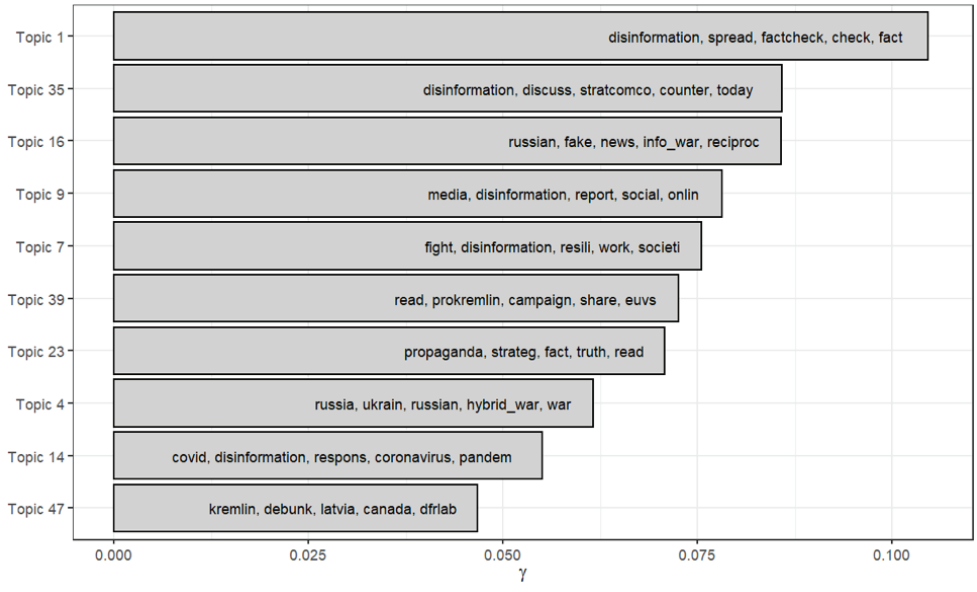

Figure 6: Top ten topics by prevalence and gamma-values (γ) that measure their levels of contribution to each topic

A longitudinal topic frequency analysis of Topic 1 shows that the keyword 'disinformation' indeed enters the NATO lexicon after the Russian military involvement in Ukraine. However,

[50] In computational linguistics, an n-gram is a continous sequence of 'n-items' (letters, words) that form a part of speech or text. Often, n-grams are used for 'stemming', reducing words to their simplest base. For example, words 'attacked', 'attacking', 'attacker' derive from the n-gram stem 'attac_'. Marc Damashek, "Gauging Similarity with N-Grams: Language-Independent Categorization of Text," *Science* 267, no. 5199 (1995): 843–48.

we observe a clear difference between NATO official texts (web) that don't prefer this term and NATO tweets that overwhelmingly rely on it. The peak in early 2014 is followed by a second peak after late 2016, possibly owing to the US elections, reaching its all-time peak in 2020, predictably due to COVID-related concerns. Topic 4 demonstrates how Russian involvement in Ukraine, as well as the 'hybrid war' narrative, becomes less popular over time. Despite its significant salience in NATO tweets and a slight reference in its documents in 2014, these references largely disappear from NATO's discursive attention zone by 2016.

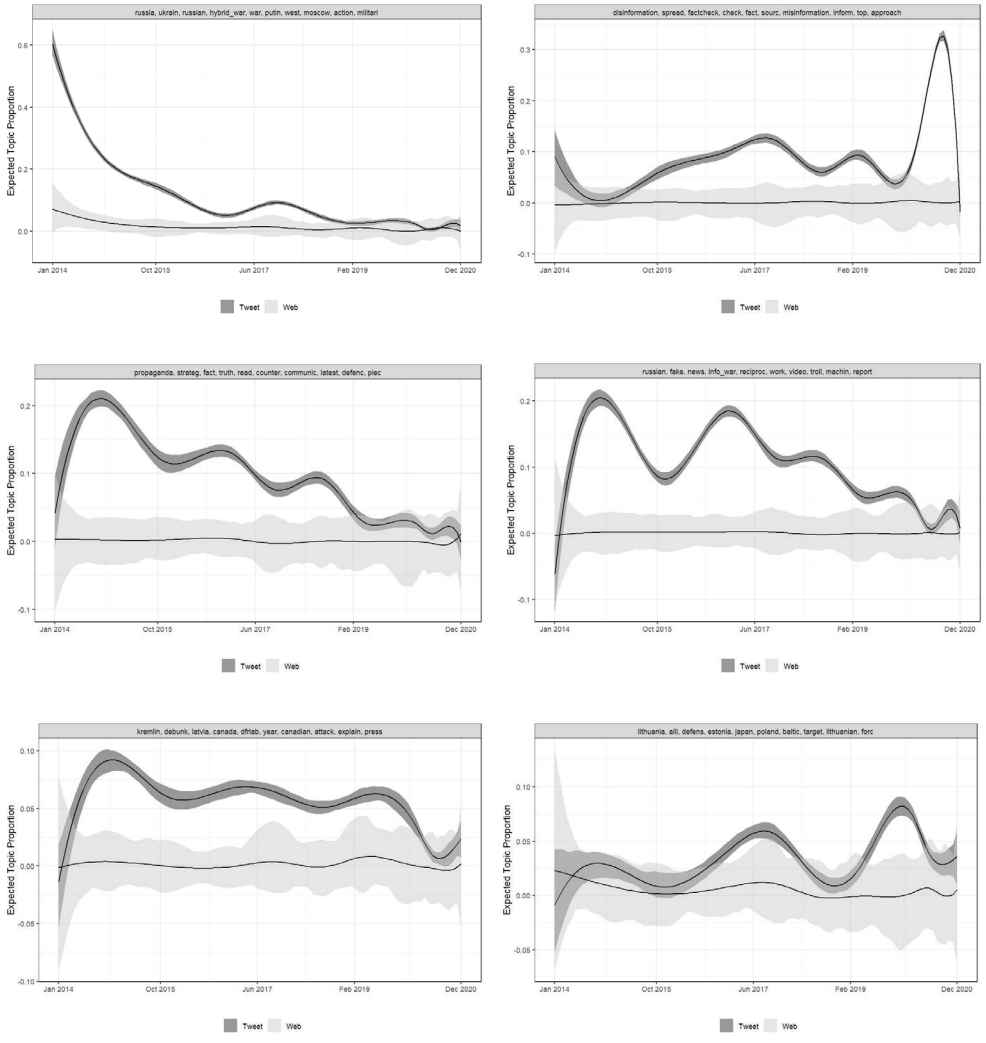

Figure 7: Longitudinal temporal frequencies of 6 highest-salience topic models

The tendency to pinpoint Russia in statements containing the keywords 'fake news', 'troll', and 'information warfare' is once again clearest in tweets as opposed to official statements, as seen in Topic 16. This tendency peaks once during the Russian military operation in Ukraine, peaks a second time around the US elections in 2016, gradually disappears from NATO's Twitter focus after 2017, and exhibits a brief third peak around the poisoning of Sergei and Yulia Skripal in Salisbury, UK, in March 2018. The same goes for Topic 23, which focuses on terms correlated with 'propaganda'. It peaks with the Russian involvement in Ukraine, marking a second brief peak around the US elections in 2016 and a third peak around the Skripal poisoning incident in 2018, later disappearing from the NATO lexicon. Regarding NATO's reference to the Baltics and Germany as potential vulnerabilities against disinformation and hybrid war, Topic 30 produces a more varied picture. Here, we observe a significant and comparable activity within NATO tweets and official documents alike. Both NATO tweets and official documents follow similar curves around the same periods (Ukraine war, US elections in 2016, Skripal poisoning, and COVID onset in March 2020), suggesting that such geographic vulnerabilities aren't new and carry on with significant strategic baggage from the past. Indeed, as Topics 47 and 49 also demonstrate, concerns and vulnerabilities around Canada, Lithuania, Estonia, Poland, and the Baltic states are emphasized continuously both in NATO official documents and in tweets.

To sum up, NATO's discourse on disinformation presents a discursive continuity and is broadly in line with its securitization preferences prior to the popularization of the terms 'fake news' or 'information operations'. By leveraging a buzzword that has mainstream popularity, NATO's discursive efforts refocus the alliance's strategic agenda back on Russia, and semantically clusters these securitization moves on existing competition areas with Moscow. Since securitization is the process by which regular events, actors, and phenomena are elevated into a policy frame that requires special measures, NATO's disinformation discourse directly fits into the theoretical spectrum. NATO's 2018 Brussels Summit Declaration and 2019 London Declaration both prioritized disinformation as a major strategic-level alliance threat, and combating information warfare has been integrated into NATO military exercises since 2017. NATO has been running wargames that focus on coordinated Russian-origin disinformation campaigns against NATO battlegroups in Latvia, Lithuania, and Poland, and has been investing in the establishment of new digital countermeasure labs.[51] In other words, as a successful securitization effort, disinformation has been receiving ample attention, resources, and cohesion-building initiatives within the NATO framework. As part of this strategy, NATO's securitization efforts have a clear securitizing agent (alliance), existential threat (Russian-origin information warfare), a referent object (alliance cohesion, electoral integrity), and an audience (international public opinion), along with new doctrinal changes and investment schemes.

5. Discussion and Conclusion

Our analysis has shown that NATO has developed different disinformation-related communication strategies for two outlets: a more up-to-date and faster-developing threat discourse for its Twitter presence, and a more traditional, slow-moving threat presence visible in its official documents. This is particularly interesting and acutely visible in other

[51] "NATO's Approach to Countering Disinformation: A Focus on COVID-19", North Atlantic Treaty Organization, 17 July 2020, https://www.nato.int/cps/en/natohq/177273.htm.

20th century military topics like command and control cohesion, missile defense, air defense architecture, naval defense, satellites, and military intelligence-related topics that are more frequently mentioned in official documents and much less referenced on Twitter. However, the overwhelming majority of disinformation, misinformation, hybrid war, information warfare, and fake news-related communication topics are securitized on Twitter. This shows the emergence of two NATO discourses: one for its official documents, and one for its social media presence and messaging.

The advent of digital communication technologies and social media has been significant for the evolution of securitization. Since securitization entails the production and dissemination of insecurity frames through discursive networks, a more dynamic, interconnected information ecosystem is more conducive for collective meaning-making. On social media, the formation of insecurity processes are more rapid and interactive, and are able to influence and alter the traditional, boring securitizing acts of elites. To that end, media outlets like Twitter provide a more interactive and fast-paced securitizing environment where elites and non-elites can set the security agenda and mobilize the masses. The most clear expression of this novel medium, as demonstrated in our results, is that NATO's Twitter securitization efforts change much faster, and spread more widely than traditional outlets like official speeches, texts, and reports.

This could be interpreted in two ways: first, NATO may prefer securitizing disinformation exclusively on Twitter, since such threats are generally more visible and debated on social media platforms. The second interpretation is that NATO's official statements and documents could largely be focusing on macro-level doctrinal issues, which pose a direct military security threat to its members, rather than disinformation, which is a nuisance but poses no direct military threat. Since disinformation is being discussed in contemporary policy debates within the context of electoral integrity and social polarization, their actual military relevance may not be salient enough to be taken into account in formal NATO documents. In either case, our study of the NATO lexicon demonstrated that disinformation and related terms are constructed as uniquely 'Russian' nuisances. This isn't surprising since most of these terms, or at least their digital interpretations, have entered the NATO lexicon after the Russian military involvement in eastern Ukraine and Crimea. However, since then, Russia remained the only country against which NATO has constructed its disinformation narratives, indicating that Russia is NATO's sole disinformation concern. Although very recently China has emerged as a runner-up country within the context of COVID-related disinformation concerns, Russia is largely the main threat in NATO's lexicon. This could be counterproductive to long-term NATO efforts to combat disinformation, given the global prevalence of fake news and information meddling. While Russian disinformation efforts are observably valid, cornering a universal problem like disinformation into the limited space of NATO's interactions with a single country may lead to conceptual contraction. This, in turn, may prevent NATO from mobilizing full alliance resources against disinformation, defined as a global and universal problem.

Overall, our analysis has shown that NATO still defines its security identity against Russia, and there has not been a significant shift in NATO's securitization dynamics since the Cold War, as evidenced by our comparative analysis of older and newer NATO texts. Although Chinese disinformation attempts have also begun to enter NATO's threat-related language, the organization's primary discursive security identity continues to develop against

and around Russia. This is most evident in our longitudinal analysis of the pre- and post-2014 documents that similarly prioritize Russia as a threat, implying that it is not really the disinformation or fake news agenda that is rendering Russia a threat for NATO. This bolsters the hypothesis that even if technologies change, the NATO-Russia rivalry will remain securitized in the same way. In other words, the contemporary disinformation and fake news agenda is a continuation of the same NATO-Russia rivalry – at least in discursive form – through newer mediums.

Bibliography

Andrejevic, Mark. *Infoglut: How Too Much Information Is Changing the Way We Think and Know*. New York: Routledge, 2013.

Balzacq, Thierry, Sarah Léonard, and Jan Ruzicka. "'Securitization' Revisited: Theory and Cases." *International Relations* 30, no. 4 (2016): 494–531.

Baum, Matthew A., and Philip B. K. Potter. "Media, Public Opinion, and Foreign Policy in the Age of Social Media." *The Journal of Politics* 81, no. 2 (2019): 747–56.

Baumann, Mario. "'Propaganda Fights' and 'Disinformation Campaigns': The Discourse on Information Warfare in Russia-West Relations." *Contemporary Politics* 26, no. 3 (2020): 288–307.

Bennett, W. Lance, and Steven Livingston. "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions." *European Journal of Communication* 33, no. 2 (2018): 122–39.

Bouvier, Gwen, and David Machin. "Critical Discourse Analysis and the Challenges and Opportunities of Social Media." *Review of Communication* 18, no. 3 (2018): 178–92.

Bradshaw, Samantha, and Philip N. Howard. "The Global Organization of Social Media Disinformation Campaigns." *Journal of International Affairs* 71, no. 1.5 (2018): 23–32.

Buzan, Barry, and Ole Wæver. "Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory." *Review of International Studies* 35, no. 2 (2009): 253–76.

Buzan, Barry, Ole Wæver, and Jaap De Wilde. *Security: A New Framework for Analysis*. UK ed. edition. Boulder, CO: Lynne Rienner Publishers, 1998.

Cour, Christina la. "Theorising Digital Disinformation in International Relations." *International Politics* 57, no. 4 (2020): 704–23.

Damashek, Marc. "Gauging Similarity with N-Grams: Language-Independent Categorization of Text." *Science* 267, no. 5199 (1995): 843–48.

DiMaggio, Paul. "Adapting Computational Text Analysis to Social Science (and Vice Versa)." *Big Data & Society* 2, no. 2 (2015). doi: https://doi.org/10.1177/2053951715602908.

Duyn, Emily Van, and Jessica Collier. "Priming and Fake News: The Effects of Elite Discourse on Evaluations of News Media." *Mass Communication and Society* 22, no. 1 (2019): 29–48.

Farkas, Johan, and Jannick Schou. "Fake News as a Floating Signifier: Hegemony, Antagonism and the Politics of Falsehood." *Javnost - The Public* 25, no. 3 (2018): 298–314.

Freelon, Deen, and Chris Wells. "Disinformation as Political Communication." *Political Communication* 37, no. 2 (2020): 145–56.

Galeotti, Mark. "The Mythical 'Gerasimov Doctrine' and the Language of Threat." *Critical Studies on Security* 7, no. 2 (2019): 157–61.

Giles, Jim. "Computational Social Science: Making the Links." *Nature News* 488, no. 7412 (2012): 448.

Grinberg, Nir, Kenneth Joseph, Lisa Friedland, Briony Swire-Thompson, and David Lazer. "Fake News on Twitter during the 2016 U.S. Presidential Election." *Science* 363, no. 6425 (2019): 374–78.

Guess, Andrew M., and Benjamin A. Lyons. "Misinformation, Disinformation, and Online Propaganda." In *Social Media and Democracy: The State of the Field, Prospects for Reform*, edited by Joshua A. Tucker and Nathaniel Persily, 10–33. SSRC Anxieties of Democracy. Cambridge: Cambridge University Press, 2020.

Hong, Liangjie, and Brian D. Davison. "Empirical Study of Topic Modeling in Twitter." In *Proceedings of the First*

Workshop on Social Media Analytics, 80–88. SOMA '10. New York, NY, USA: Association for Computing Machinery, 2010.

Jack, Caroline. "Lexicon of lies: Terms for problematic information." *Data & Society* 3, no. 22 (2017): 1094–096.

Jr, Edson C. Tandoc, Zheng Wei Lim, and Richard Ling. "Defining 'Fake News.'" *Digital Journalism* 6, no. 2 (2018): 137–53.

Khaldarova, Irina, and Mervi Pantti. "Fake News." *Journalism Practice* 10, no. 7 (2016): 891–901.

Knudsen, Olav F. "Post-Copenhagen Security Studies: Desecuritizing Securitization." *Security Dialogue* 32, no. 3 (2001): 355–68.

Krippendorff, Klaus. "Measuring the Reliability of Qualitative Text Analysis Data." *Quality and Quantity* 38, no. 6 (2004): 787–800.

Kurowska, Xymena and Anatoly Reshetnikov. "Neutrollization: Industrialized Trolling as a Pro-Kremlin Strategy of Desecuritization." *Security Dialogue* 49, no. 5 (2018): 345–63.

Lanoszka, Alexander. "Disinformation in International Politics." *European Journal of International Security* 4, no. 2 (2019): 227–48.

Liang, Hai, and King-wa Fu. "Testing Propositions Derived from Twitter Studies: Generalization and Replication in Computational Social Science." *PLOS ONE* 10, no. 8 (2015). doi: https://doi.org/10.1371/journal.pone.0134270.

Lipizzi, Carlo, Dante Gama Dessavre, Luca Iandoli, and Jose Emmanuel Ramirez Marquez. "Towards Computational Discourse Analysis: A Methodology for Mining Twitter Backchanneling Conversations." *Computers in Human Behavior* 64 (2016): 782–92.

Lysenko, Volodymyr, and Catherine Brooks. "Russian Information Troops, Disinformation, and Democracy." *First Monday* 23, no. 5 (2018). doi: https://doi.org/10.5210/fm.v22i5.8176.

Mälksoo, Maria. "Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO." *European Security* 27, no. 3 (2018): 374–92.

Marchi, Anna, and Charlotte Taylor, eds. *Corpus Approaches to Discourse: A Critical Review*. 1st edition. New York: Routledge, 2018.

Mas-Manchón, Lluís, Frederic Guerrero-Solé, Xavier Ramon, and Laura Grande. "Patriotic Journalism in Fake News Warfare: El País' Coverage of the Catalan Process." *The Political Economy of Communication* 8, no. 2 (2021). http://www.polecom.org/index.php/polecom/article/view/123.

Maweu, Jacinta Mwende. "'Fake Elections'? Cyber Propaganda, Disinformation and the 2017 General Elections in Kenya." *African Journalism Studies* 40, no. 4 (2019): 62–76.

Mejias, Ulises A, and Nikolai E Vokuev. "Disinformation and the Media: The Case of Russia and Ukraine." *Media, Culture & Society* 39, no. 7 (2017): 1027–42.

Monsees, Linda. "'A War against Truth' - Understanding the Fake News Controversy." *Critical Studies on Security* 8, no. 2 (May 3, 2020): 116–29.

Morgan, Susan. "Fake News, Disinformation, Manipulation and Online Tactics to Undermine Democracy." *Journal of Cyber Policy* 3, no. 1 (2018): 39–43.

Neo, Rick. "When Would a State Crack Down on Fake News? Explaining Variation in the Governance of Fake News in Asia-Pacific." *Political Studies Review* (2021). doi: https://doi.org/10.1177%2F14789299211013984.

Polletta, Francesca, and Jessica Callahan. "Deep Stories, Nostalgia Narratives, and Fake News: Storytelling in the Trump Era." In *Politics of Meaning/Meaning of Politics: Cultural Sociology of the 2016 U.S. Presidential Election*, edited by Jason L. Mast and Jeffrey C. Alexander, 55–73. Cultural Sociology. Cham: Springer International Publishing, 2019.

Renz, Bettina. "Russian Military Capabilities after 20 Years of Reform." *Survival* 56, no. 3 (2014): 61–84.

Roberts, Margaret E., Brandon M. Stewart, D. Tingley, and E. Airoldi. "The Structural Topic Model and Applied Social Science." In *ICONIP2013*. Daegu, South Korea, 2013. https://scholar.princeton.edu/files/bstewart/files/stmnips2013.pdf.

Roberts, Margaret E., Brandon M. Stewart, Dustin Tingley, Christopher Lucas, Jetson Leder-Luis, Shana Kushner Gadarian, Bethany Albertson, and David G. Rand. "Structural Topic Models for Open-Ended Survey

Responses." *American Journal of Political Science* 58, no. 4 (2014): 1064–082.

Roberts, Margaret E., Brandon M. Stewart, and Dustin Tingley. "Stm: An R Package for Structural Topic Models." *Journal of Statistical Software* 91, no. 1 (2019): 1–40.

Ross, Andrew S., and Damian J. Rivers. "Discursive Deflection: Accusation of 'Fake News' and the Spread of Mis- and Disinformation in the Tweets of President Trump." *Social Media + Society* 4, no. 2 (2018). doi: https://doi.org/10.1177/2056305118776010.

Saurwein, Florian, and Charlotte Spencer-Smith. "Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe." *Digital Journalism* 8, no. 6 (July 2, 2020): 820–41.

Sinovets, Polina, and Bettina Renz. "Russia's 2014 Military Doctrine and beyond: Threat Perceptions, Capabilities and Ambitions." NATO Research Papers. Rome: NATO Defense College, July 2015. https://www.ndc.nato.int/news/news.php?icode=830.

Smith, Christopher A. "Weaponized Iconoclasm in Internet Memes Featuring the Expression 'Fake News.'" *Discourse & Communication* 13, no. 3 (2019): 303–19.

Stritzel, Holger, and Sean C Chang. "Securitization and Counter-Securitization in Afghanistan." *Security Dialogue* 46, no. 6 (2015): 548–67.

Tan, Netina. "Electoral Management of Digital Campaigns and Disinformation in East and Southeast Asia." *Election Law Journal: Rules, Politics, and Policy* 19, no. 2 (2020): 214–39.

Tong, Chau, Hyungjin Gill, Jianing Li, Sebastián Valenzuela, and Hernando Rojas. "'Fake News Is Anything They Say!' — Conceptualization and Weaponization of Fake News among the American Public." *Mass Communication and Society* 23, no. 5 (2020): 755–78.

Tucker, Joshua, Andre Guess, Pablo Barberá, Cristian Vaccari, Alex, ra Siegel, Sergey Sanovich, Denis Stukal, Brendan Nyhan. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature." *Hewlett Foundation* (blog), March 19, 2018. https://hewlett.org/library/social-media-political-polarization-political-disinformation-review-scientific-literature/.

Wang, Hongning, Duo Zhang, and ChengXiang Zhai. "Structural Topic Model for Latent Topical Structure Analysis." Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies, Portland, Oregon, June 19-24, 2011.

Wallach, Hanna M. "Topic Modeling: Beyond Bag-of-Words." In *Proceedings of the 23rd International Conference on Machine Learning*, 977–84. ICML '06. New York, NY, USA: Association for Computing Machinery, 2006. https://doi.org/10.1145/1143844.1143967.

Williams, Michael C. "Words, Images, Enemies: Securitization and International Politics." *International Studies Quarterly* 47, no. 4 (2003): 511–31.