Lund University
Department of Political Science
Peace and Conflict Studies

FKVK02
VT21
Supervisor: Daniel Møller Ølgaard

From Crimea to Covid:

The EU’s changing perspective on Russian disinformation from 2015-2021

Word Count: 9134

Ellen Andreasson

Abstract

We are currently living in the information age. Our social media news feeds are constantly filled with updates from our friends and family, but also with news and findings from all around the world. With these massive information flows, it is becoming harder to fact check. Actors, such as Russia, have used the new information environment to their advantage, by spreading disinformation campaigns. Simultaneously as social media has grown in popularity, tensions between Russia and the European Union have increased. The Russian annexation of Crimea in 2014 especially complicated the relationship, with agreements paused and EU sanctions imposed. In 2015, the EU started to actively address the issue of disinformation and have since published multiple strategies regarding disinformation. Using the discourse analysis "What is the Problem Represented to Be" and the theory of securitization, this thesis will explore how the perception of Russian disinformation as a threat has changed in EU's discourse from 2015 to 2021. By analyzing six documents on disinformation published by the EU using these tools, a gradual securitization of Russian disinformation can be identified where the EU has adapted its threat perception to other challenges, such as democratic elections and the Covid-19 pandemic.

Key words: Russia, the European Union, WPR, EEAS, disinformation, discourse analysis, securitization.
Antal ord: 9134

Table of Contents

Abbreviations

EU: European Union

EEAS: European External Action Service

MH17: Malaysia Airlines Flight 17

NATO: North Atlantic Treaty Organization

WPR: What is the problem represented to be?

1 Introduction

"I have to say, to finish Ms President that unhappily I see a worrying trend of Russian authorities that seem to be choosing to deliberately deepen confrontation with the West, with us, including through attacks with disinformation and other negative activities" (Borell 2021).

This was said by the EU's High Representative, Josep Borell, at the European Parliament debate in April 2021. Borell, being the head of the European External Action Service (EEAS), expresses a concern that has increasingly been making headlines: Russian disinformation campaigns. Since 2015, when the European Council expressed a need to address Russian disinformation campaigns, the EU has actively tackled disinformation. Working with the EEAS, the EU has countered disinformation by publishing different strategies, reports and establishing the East Stratcom Task Force, whose main task is raising awareness of pro-Kremlin disinformation (EEAS 2019b).

Why has Russian disinformation received so much attention? With the rise of the internet, there has been an increased availability of information. A considerable amount of our questions can be answered through a simple Google Search. The internet has also led to the establishment of social media, where information is posted and shared constantly. With the increasing flow of information it is, however, becoming harder to fact check (Shu et al. 2020b:1-2). Some actors, such as Russia, have used the information environment on the internet to their advantage, by spreading disinformation campaigns that promote certain narratives (Orenstein 2019:136). Simultaneously, tensions have risen between the EU and Russia. The annexation of Crimea in 2014 resulted in paused agreements and EU sanctions (EEAS 2021a.) Most recently, the Covid-19 pandemic that spread globally in 2020 has led to new disinformation flows, and the EU has identified several Russian disinformation campaigns that undermine the EU strategy concerning the pandemic (EEAS 2021b).

Have these factors caused the EU to regard Russian disinformation as an existential threat? To investigate how the EU's perception of Russian disinformation has changed throughout the years, I have studied the EEAS discourse from 2015 until now. The thesis begins with a background section, where a deeper historical discussion of disinformation and the EU-Russia relationship is presented. The methodology is then introduced, with the discourse analysis approach “What is the Problem Represented to Be?” (Bacchi 2009). Six documents from the EEAS and the European Commission are analyzed using the WPR approach. The results are lastly discussed using the theory of securitization in order to understand how the European Union’s perception of Russian disinformation as a threat changed in the EU’s discourse since 2015.

1.1 Aim & Research Question

The aim of this thesis is to analyze how Russian disinformation has been represented as a threat for the EU in its discourse since 2015, which was when the EU started to actively address disinformation (EEAS 2019b). Specifically, I want to study how the EU’s discourse has changed regarding Russian disinformation. By studying the time period 2015 to 2021, an understanding can be made of how different contemporary and historical events, such as the Russian annexation of Crimea 2014, various democratic elections and referendums, and the Covid-19 pandemic, have shaped the perception of Russian disinformation. By mainly studying documents published by the European External Action Service (EEAS), which is the EU’s diplomatic and foreign defense service, the aim is to show whether there has been any change in how the EEAS frames the threat of Russian disinformation. The discourse analysis “What is the Problem Represented to Be” will assist me in reaching this aim (Bacchi 2009). First, I will explore how the EEAS presents Russian disinformation, then identify underlying assumptions, and lastly study the genealogy of the representation. I will then discuss my findings by applying the securitization theory, to see if there has been a change within the security discourse. With this approach, my aim is to see if the securitization of Russian disinformation can be connected to general tensions in the EU-Russia relationship caused by various political or global events. Thus, the question I want to answer is:

How has the European Union’s perception of Russian disinformation as a threat changed in the EU’s discourse from 2015 to 2021?

2 Background

2.1 Disinformation as a Security Threat

Disinformation is generally understood as false information that is deliberately spread to change the opinion of the public. Although the concept of disinformation is highly connected to social media in today's political rhetoric, disinformation has been around long before the internet existed. The term "disinformation" originates from the Russian word "dezinformatsiya". Dezinformatsiya was first coined by the KGB, which was the Soviet Union's security agency, as a word for propaganda. The Soviet Union would use disinformation campaigns as a way to influence their opponents by reaching out to their citizens through foreign media (Boghardt 2009:2). A well-known example of one of KGB's disinformation campaigns is "operation INFEKTION" in the 1980s. The campaign spread information which claimed that the United States had invented the AIDS epidemic as a biological weapon (Stengel 2019:140).

Disinformation is often classified as a type of hybrid warfare (Hedling 2021:845). Hybrid warfare combines irregular and conventional military strategies that includes virtual tactics, such as cyberattacks on electronic infrastructure or hacking with the aim to release vulnerable information (Orenstein 2019 :39). The reason why disinformation can be seen as an effective tactic in warfare is because it causes worry and questions from the citizens who are the target of the campaign. Disinformation can thus be seen as a type of psychological warfare as it aims at affecting individuals' psyche, such as their belief system and emotions (Doroszczyk 2018:522,525). By spreading information that might question a country's government or politicians, or other political issues, citizens themselves may start to question the people who run their country. Therefore, disinformation becomes an effective tactic for states to create instability and questioning from inside of their target country. Disinformation is also a much cheaper war tactic than traditional means, such as military tanks or soldiers (Stengel 2019:3-5).

The rise of the internet has caused a major increase in information flows. Information is now accessible in seconds, and our news feeds are constantly updated with information about our friends and family, as well as news stories from all around the world. It has made us more globally connected and aware than ever before (Shu et al. 2020a:2-3). However, while there are many positive aspects of the internet and social media there are also negative side effects, such as an increased amount of disinformation. A vast number of users are starting to rely on social media instead of traditional media outlets for news, contributing to the increased spread of disinformation. With the overflow of information, it is harder to fact check and be source critical, making social media users more vulnerable to disinformation campaigns (Shu et al. 2020b:1-2).

Disinformation is difficult to counter on social media, as it is hard to detect. The posts are usually disguised as “real” news articles and tend to be purposefully controversial, which brings more attention and engagement to the content, spreading it to more users. Yet another factor that contributes to the problem of disinformation on social media is filter bubbles. Filter bubbles are results of algorithms that are especially customized to the user’s interests and are prevalent on most social media platforms. The filter bubbles often lead to the user only being shown one or a few perspectives on a subject, making the user more vulnerable to disinformation that reinforces their own views (Shu et al. 2020a:4). Disinformation is also a difficult threat for democracies to tackle. A key principle of democracies is freedom of speech, and prohibiting certain information on the internet is therefore a challenge for democratic societies as it could be seen as a type of censorship. Therefore, it is hard for democratic organizations, such as the EU, to implement disinformation policies which prohibit certain content (Stengel 2019:2).

2.2 The Russia-EU Relationship

To examine how the EU’s perception of Russian disinformation has changed, it is necessary to be aware of the two powers' historical relationship. After the dissolution of the Soviet Union in 1991, Russia and the EU attempted to create a more stable relationship. The powers have reason for wanting to cooperate on both economic and geopolitical levels. Both have valuable resources; Russia is a huge exporter of energy in the form of fossil fuels, and the EU has a market with consumers that are important for Russia. Since Russia and the EU are the two largest powers in the geographical area, their cooperation is also necessary for keeping peace and stability in Europe (EEAS 2021a). Even though the initial relationship between the EU and Russia was relatively stable, the powers did see strains in their relationship. Some of these issues are related to the EU's close connection to the North Atlantic Treaty Organization (NATO). One example is the Kosovo independence of 2008, where Russia showed support for Serbia (against independence) while a majority of EU member states and NATO supported independence (Hughes 2013:1010-1011). NATO and the EU have also previously cooperated on defense strategies and share a majority of member states (NATO 2021). Russia, who has historically seen NATO as a threat because of their affiliation with the US, was, especially after the Kosovo independence, starting to categorize the EU together with NATO as being a national security threat (Hughes 2013:1000). NATO and the EU represent a geographical threat to Russia, as both organizations have expanded to the Russian neighborhood, potentially constricting Russia's power in the area (Orenstein 2019:17). Disinformation campaigns have pointed at this relationship, with some sources claiming that it is a way of spreading Western or American propaganda (Orenstein 2019:24-26). The relationship between Russia and the EU became even more strained with the Russian annexation of Crimea in 2014. The annexation, which the EU condemns to be illegal, resulted in EU sanctions oriented toward Russia, and several frozen cooperation agreements (EEAS 2021a). In sum, events, such as the Kosovo independence and the annexation of Crimea, has increased the tensions between the EU and Russia.

2.3 Previous Research

While disinformation has long been a topic of interest within international relations, the subject has become growing topic of interest during the last few years. A reason for the increased interest is the US election of 2016, where the involvement of Russian disinformation made headlines all around the world. The accusations of Russian involvement, however, is not the only reason for why disinformation became a subject of interest for the public after the 2016 US election (Orenstein 2019:10). The American president Donald Trump became an avid user of the term “fake news”, which contributed to a larger discussion on the controversy of disinformation as a threat (Stengel 2019:290).

The relationship between Russia and the EU is a subject that has been widely discussed within peace and conflict studies. As noted, Russia and the EU have had a rocky relationship for a long time, which has resulted in a substantial amount of research concerning their different policy areas. Research about Russian disinformation and the EU, however, has mostly been conducted during the past few years, starting from around 2016 and onwards. Most has to do with the Russian annexation of Crimea in 2014, which resulted in the EU publicly responding to Russian disinformation by establishing the East Stratcom Task Force. A vast amount of the research conducted describes specific cases, such as the Russian disinformation threat during COVID-19, during the European Parliament Elections of 2019 or case studies of member states (Sukhankin 2020; Kovalčíková & Tabatabai 2020; Magdin 2020). Other research is focused on what actions the EU has taken in tackling the problem of Russian disinformation. Elsa Hedling, for example, has discussed how the EEAS has adapted to the new information climate, moving from traditional means of EU-diplomacy (Hedling 2021).

While the topic of Russian disinformation and the EU has received more attention recently, few of the publications on EU and Russian disinformation give an in-depth analysis of in what way the EU’s discourse of the threat has escalated since the 2014 annexation. By focusing on documents published by the EEAS during the time period 2015-2021 I hope to fill this research gap. Using a discourse analysis, particularly Carol Bacchi’s “what is the problem represented to be” (WPR) approach, I am aiming to contribute to the subject by studying the meaning behind the discourses in the EEAS documents. By studying the meanings and genealogy of the problem representations, my contribution to the research on Russian disinformation will be made by connecting the framing of the discourses to contemporary and historical events.

3 Theory

3.1 Securitization

An important part of my research question is threat perception. The notion of "threat perception" will be understood using securitization. The theory of securitization has its roots in the Copenhagen school, with theorists such as Barry Buzan making meaningful contributions in developing the theory by pointing out its advantages in broadening the concept of security. By using securitization, anything can be constructed as a threat, which goes beyond traditional notions of security such as military capabilities or polarity (Sjöstedt 2017:3). The theory of securitization is used in the "discussion" section in order to understand how the EU's framing of Russian disinformation as a threat has changed.

Securitization describes the process where an issue moves from "normal" political discourse to being seen as and accepted as a threat. A "securitizing move" is when the issue is presented as a threat to a referent object (Sjöstedt 2017:3). By the issue being presented as a threat in the political discourse it legitimizes action to counter the threat, by means that are not normally a part of the "political procedure" (Buzan et. al, 1998:23-24). Barry Buzan, Ole Wæver and Jaap de Wilde describe securitization as a "speech act" where, similar to discourse analysis, language is the decisive factor that moves an issue to the security agenda (Buzan et. al, 1998:26). Securitization is also closely related to theories of framing, since it describes how an issue is framed, using discourse, as a security threat (Sjöstedt 2017:3). In order for an issue to be seen as an existential threat, it is necessary that an important securitizing actor sees and frames it as such (Floyd 2013:24). Although the theory does not specify precisely who can be identified as a securitization actor, it is presumed that the actor has authoritative power. Politicians, NGO:s, or multilateral institutions such as the EU can therefore be seen as important actors (Sjöstedt 2017:3). The securitization process, however, is not truly complete until the audience accepts it as such (Buzan et al, 1998:25). The audience is identified by who the securitizing actor is connected to, and who they frame is threatened by the issue, but could for example be the general public (Sjöstedt 2017:3). Securitization, in sum, describes a change in discourse where an issue is presented and discussed in terms of security rather than normal political discourse (Floyd 2013:24). By applying securitization on the EU's discourse regarding Russian disinformation from 2015 to 2021, different securitization moves can be identified, showing that their perception of Russian disinformation as a threat has changed.

4 Methodology

4.1 Definiton of Disinformation

In order to study disinformation, it is necessary to conceptualize the phenomenon. Disinformation is a concept that can be difficult to define. This is because the concept is rather hard to identify, especially since it is often confused with concepts such as misinformation, propaganda and fake news. Misinformation is the spread of false information, but it does not imply that the information is spread deliberately or with a certain intent. Disinformation, however, is defined by the EU as “verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public” (European Commission 2021). This thesis focus is disinformation rather than misinformation since its focus is the EUs perception of Russia’s deliberate attempts at spreading false information. I will be using the EU definition of disinformation since I am analyzing disinformation from the EUs perspective. Therefore, it is useful to use their definition of the concept rather than other definitions of disinformation since it gives insight on how they view the concept.

4.2 Discourse Analysis

I will analyze how the EU has securitized Russian disinformation since 2015 by using a discourse analysis. A discourse analysis, similar to securitization, is qualitative and focuses on how language creates meaning, taking into account broader power relations and context that could have an effect on the discourse (Halperin & Heath 2017:335). Discourse analysis has its roots in constructivism, as it believes that “meanings are socially and discursively constructed” (Halperin & Heath 2017:337). Discourse analysis is also a fitting method with the choice of theory for this thesis, securitization, since securitization itself is considered a speech act and is largely based on the conception that language creates meaning.

4.2.1 What is the Problem Represented to Be?

Discourse analysis is an umbrella term which has many different approaches depending on what material is analyzed and what aim or perspective the researcher wants to explore (Jørgensen & Phillips 2011:24). The approach that will be used in this thesis is based on Carol Bacchi's "what is the problem represented to be?" (WPR). Bacchi's approach is adjusted and geared towards the analysis of policy documents, which makes WPR helpful for my study as most of my material consists of EU policy documents and reports. WPR is a social-constructivist approach, which implies that it is more focused on how meaning is produced by social forces (Bacchi 2009:33) The approach is critical, meaning that it aims to explain and discover aspects of power in discourses that are usually taken for granted (Bacchi 2009:39). The purpose of WPR is to uncover how problems are presented in policies, and identifying contexts and other factors that may affect how the issue was presented in the policy. The approach also recognizes that the actor that publishes the policy has great power in shaping how the issue is presented. Bacchi means that by using WPR on policies, it uncovers how the problem is thought about (Bacchi 2009:1). The WPR approach is helpful in answering my research question as it will help me identify how the EEAS has shaped the issue of Russian disinformation since the annexation of Crimea in 2014. It will also help me understand other contexts or assumptions that could have contributed to the framing of the issue in the policies.

In order to uncover the different power dynamics and context that may affect how a problem is presented in a policy, Bacchi uses six questions to answer when analyzing policies. These are:

1. What is the problem represented to be in a specific policy?
2. What presuppositions or assumptions underlie this representation of the problem?
3. How has this representation of the problem come about?
4. What is left unproblematic in this problem representation?
5. What effects are produced by this representation of the problem?

6. How is this representation of the problem produced, disseminated and defended? How could it be questioned, disrupted and replaced?

I have chosen to answer the first three questions in my analysis. The last three questions are aimed at disclosing and problematizing different power relationships in policy documents. Since I am more interested in understanding how the policies view a certain problem, the first three questions are more relevant. The first question will help identify how the issue of disinformation is discussed, while the second and third question will be used to explain connections to the EU-Russian relationship in general, as well as how events in 2015 to 2021 have shaped the discourse. The three questions will be applied to the documents that I have chosen for each time period to better understand the EEAS perception of Russian disinformation as a threat over time.

Bacchi describes the first question as fairly straightforward, as it is solely used to identify different problem representations that can be found in the policies (Bacchi 2009:2). One way to spot problem representations is by seeing what the policy states has changed and needs to be addressed or looking at where funding is spent (Bacchi 2009:55,4).

The second question seeks to understand if there are any assumptions in the policy that are needed in order to understand the problem representation. The question aims at realizing that there may be cultural values that have framed the issue. In this question, Bacchi suggests looking for three different forms of discourse analysis: binaries, key concepts and categories. Binaries are identified by analyzing how two sides are presented, and which side is considered to be superior (Bacchi 2009:7). Key concepts are identified by seeing how terms, such as disinformation or hybrid threats, are given meaning in policies. Key concepts, however, can be hard to understand because most of them are deeply rooted in culture, history and institutions, making it difficult to identify them (Bacchi 2009:8). Categories, such as classifying threats by actors, referent objects or counterstrategies, are also helpful tools to see how issues are thought about by the publishers but also how they want the public to frame the issues (Bacchi 2009:9). These different tools will be used to see how the EEAS has shaped the issue of Russian disinformation.

The third question focuses on Foucault's notion of genealogy. It seeks to uncover the context and history that has shaped the representation of the problem. It reflects on the developments that have contributed to the framing of the issue (Bacchi 2009:10). In my analysis, the third question will be used to see how events, such as the annexation of Crimea and elections during the time period, may have affected the EU's framing of Russian disinformation as a threat, as well as reflecting on the historical relationship between the EU and the Russian Federation.

4.3 Material & Scope

I have chosen to analyze the time period 2015-2021. 2015 is when the East Stratcom Taskforce was established and is cited by the EEAS as the year where the EU started actively countering disinformation (EEAS 2019b). Thus, information on the EUs strategies against disinformation is from 2015 onwards, making it a reasonable starting point for my research. To analyze the material, I have chosen to split up the material into three different time periods, each consisting of two different documents. These time periods are 2015-2016, 2017-2019 and 2020-2021. The time periods were chosen based on the material found. The publications on EU disinformation fell into these time slots because of their different focus. While the first time period focuses on the disinformation threat in general, the latter two focus on the European Parliament Elections of 2019 and the Covid-19 pandemic. Therefore, it made sense to study these time periods separately.

The material was limited mainly to documents published by the European Commission together with the EEAS. The limitation was made since the EEAS is the EU's diplomatic branch and one of their main tasks is assisting the High Representative (currently Joseph Borrell) in establishing foreign defense strategies (EEAS 2019a). Thus, counter strategies against disinformation are published in collaboration with the EEAS, making the EEAS a significant organ to study within the EU when it comes to disinformation. Six different EU documents have been chosen for the analysis. I have chosen two documents for each of the three time periods.

The first time period, 2015-2016 contains two different documents. The first, "March 2015 Council Conclusions" is the only policy that is not published together with the EEAS. The document was, however, still important to the analysis since it includes the first mention of Russian disinformation as a threat to the EU and led to the establishment of the East Stratcom Task Force (EEAS 2019b; EUvsDisinfo 2021a). The next policy is the "Joint Framework on Countering Hybrid Threats" (EEAS & European Commission 2016), which is stated by both the East Stratcom Taskforce and the EEAS as their next step in countering disinformation (EEAS 2019b; EUvsDisinfo 2021a).

For the period 2017-2019 the "Action Plan on Disinformation" (2018) is important to the analysis as it summarizes the EU's stance on Russian disinformation thus far and lays out a plan on counterstrategies (EEAS & European Commission 2018). The "Progress Report on the Action Plan against Disinformation" (2019) was chosen as it is the only document published by the EEAS and the Commission after the Action Plan and gives insight in how the EU views Russian disinformation after the European elections of 2019 (EEAS & European Commission 2019).

The last time period, 2020-2021, includes the joint communication "Tackling COVID-19 disinformation - Getting the facts rights" and the "EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic" (EEAS & European Commission 2020; EEAS 2021b). Since the time period is recent, the joint communication is the only official strategy on disinformation published by the EEAS and the European Commission found thus far. Therefore, it is complemented with the EEAS report from 2021. The report is referred to in the joint communication as a part of the EEAS strategy against disinformation (EEAS & the European Commission 2020:5). By including the EEAS report, a better understanding of the EU's discourse regarding Russian disinformation during 2021 can be made.

5 Analysis

Before analyzing the six documents, it is necessary to explain how the EU has responded to disinformation generally since 2015. To tackle the issue of disinformation, the EU turned to its diplomatic wing, the European External Action Service (EEAS). The EEAS task within the EU is to assist the High Representative for Foreign Affairs and Security Policy with issues having to do with foreign affairs and security. It works closely with other EU institutions, such as the European Commission, to carry out its work (EEAS 2019a). The EEAS has actively countered disinformation since 2015, starting by establishing the East Stratcom Task Force. The task force launched the website EUvsDisinfo the same year, where they collect data on pro-Kremlin disinformation with the goal of spreading awareness to the public on the issue of Russian disinformation (EUvsDisinfo 2021a). The EEAS has since then, together with the European Commission, published several strategies on tackling disinformation, which will be analyzed using the WPR approach.

5.1 Time Period One: 2015-2016

5.1.1 What is the Problem Represented to Be?

The first mention of Russian disinformation appears in the European Council’s document *Conclusions - 19 and 20 March 2015*. The document states a broad area of actions they want the EU to take, and discusses Russian disinformation under the subtitle “External Relations”:

> *“The European Council stressed the need to challenge Russia's ongoing disinformation campaigns and invited the High Representative, in cooperation with Member States and EU institutions, to prepare by June an action plan on strategic communication. The establishment of a communication team is a first step in this regard.”*(European Council 2015:5)

The problem representation is straightforward: the EU recognizes Russian disinformation as an issue. The Council stresses the need of establishing a communication team and encourages the EEAS to create it. Since one of EEAS main tasks is foreign defense, the issue of Russian disinformation is represented as a potential threat to the EU, needing counteracting (EEAS 2019a; European Council 2015:5).

The policy was later followed up by the *Joint Framework on Countering Hybrid Threats* (EEAS & European Commission 2016). The framework focuses on increasing awareness of hybrid threats in general, with the problem representation being the increased intelligence of technology in combination with the instability in "the EU's eastern and southern neighbourhood" (Ibid:2). The framework addresses the issue of disinformation under the subtitle "strategic communication", meaning that it can be used to "radicalise individuals, destabilise society and control the political narrative" (Ibid:4). The framework states that strategic communication using and monitoring traditional media, but especially social media, is essential. This presents social media as an additional problem when it comes to disinformation. The framework also calls on the East and Arab Stratcom Task Forces to monitor "non-EU information", giving the implication that the disinformation issue is coming from either the Eastern Neighborhood or the Arab world (Ibid:5).

5.1.2 What Presuppositions or Assumptions Underlie this Representation of the Problem?

While the European Council's conclusions are fairly straightforward, there are a number of presuppositions identified in the "Joint Framework on Countering Hybrid Threats" regarding Russian disinformation. Although Russia is not addressed directly, the framework states that "many of the current challenges to peace, security and prosperity originate from instability in the EU's immediate neighborhood" (EEAS & European Commission 2016:2). Given that the EEAS website refers to Russia as the "EU's largest neighbor", one can assume that the framework is referring to Russia as their immediate neighbor (EEAS 2021a). This is supported by the 2015 conclusions, where Russia is stated as an actor that is spreading disinformation and is seen as something that the EU needs to "challenge" (European Council 2015:5). A binary relationship is also identified between EU and non-EU countries, with the Framework stating that there needs to be greater monitoring of non-EU languages. This implicates a "us vs. them" relationship between the EU and non-EU countries, Russia being one of them (European Commission & EEAS 2016:5). Another assumption can be made concerning what the EEAS considered Russian disinformation to threaten. The concern can be identified mainly on an individual level, as the Framework states that disinformation can "radicalise individuals, destabilise society and control the political narrative" (Ibid:4). The framing of disinformation in this regard implies that the EEAS sees individuals as being the most vulnerable to disinformation, which could result in destabilisation on a societal level.

Cooperation is a key concept in the framework. The issue of hybrid threats in general, but also the issue of disinformation, is seen as a common problem needing a shared defense. Throughout the Framework, there is an emphasis on the cooperation of member states and civil society, as well as a mentioning of potentially working with NATO. The emphasis on cooperation gives the implication that hybrid threats and disinformation are broad and demand a wide amount of counter actors (EEAS & European Commission 2016:18). Placing disinformation under the wide category of hybrid threats and under a small subtitle of strategic communication, however, also gives the implication that although the EEAS may see disinformation as a threat, it is not seeing the tactic as prioritized yet- at least not in the field of hybrid threats (Ibid:4). Therefore, one can assume that disinformation is not seen by the EEAS as an urgent threat needing immediate defensive countermeasures yet, although it does regard it as a potential issue as it is setting out strategies of defense.

5.1.3 How has this Representation of the Problem Come About?

Given the complicated history of Russia's tense relationship with the West, it is not surprising that the EU may be extra cautious of potential threats coming from Russia. The Russian annexation of Crimea in 2014 is one of the reasons why the problem of disinformation started to appear on the EEAS defense agenda. The annexation is mentioned in the conclusions under the point above the mentioning of Russian disinformation, stating that "the European Council does not recognize and continues to condemn the illegal annexation of Crimea and Sevastopol by the Russian Federation". The annexation also resulted in increased attention to Russian disinformation. In the annexation aftermath, member states within the EU started to recognize disinformation campaigns promoting Russia's efforts (Ördén 2020:6).

Another event that could have enhanced the EEAS' view on Russian disinformation as a threat is the Malaysia Airlines Flight 17 (MH17) in 2014, that was shot down by a missile close to the Russian and Ukrainian border. While it was confirmed by the international investigation that the missile was launched from pro-Russian territory, Russian disinformation campaigns pinned it on Ukraine, saying it was an attempt to slander Russia (Orenstein 2019:36). These events, combined with the history of Russian and Soviet disinformation that have targeted the West, could have led to the increased perception of Russian disinformation as a threat, thus leading to the need to establish a counter strategy.

5.2 Time Period Two: 2017-2019

5.2.1 What is the Problem Represented to Be?

In the *Action Plan against Disinformation* (2018) the EEAS together with the European Commission sets out tactics to counter disinformation. The general problem represented in the plan is an increased concern of disinformation campaigns during the European Parliament Elections of 2019. Disinformation is presented to be a threat to democracy, as the Action Plan sets out to "protect the Union's democratic systems and combat disinformation, including in the context of the upcoming European elections" (EEAS & European Commission 2018:1). The Action Plan was, approximately six months after its publication, followed up by the *Report on the implementation of the Action Plan against Disinformation* (2019), summarizing how the implementation of the actions have worked. In both policies, the problem of Russian disinformation is stated several times. The Action Plan states that "disinformation by the Russian Federation poses the greatest threat to the EU" (EEAS & European Commission 2018:4). The report of 2019 states that "the evidence collected revealed a continued and sustained disinformation activity by Russian sources" (EEAS & European Commission

2019:3). In both cases, the Russian Federation is the only state-actor that is mentioned by name, implying that the EEAS perceives Russia as the actor contributing to the greatest threat when it comes to disinformation. Russian disinformation is further presented to be a threat to democracy and the "EU and its values" (ibid:3). This representation of Russian disinformation differs from period one, where the "Joint Framework on Hybrid Threats" did not mention Russia by name, and the 2015 European Council conclusions did not specify *how* Russian disinformation posed a threat to the EU (EEAS & European Commission 2016; European Council 2015:5). In the Action Plan and the report, however, Russia is stated as an actor and the EU and its values are clearly stated as threatened by Russian disinformation (EEAS & European Commission 2018:4; EEAS & European Commission 2019:3).

Social media is a recurring problem representation in both policies with the Action Plan saying that "social media have become important means of spreading disinformation" (EEAS & European Commission 2018:4). Although social media was represented as a problem in period one as well, the problem representation in period two is clearer. The Action Plan states more specific measures for tackling the problem, stating that the EU's needs to adapt to new technologies and tools to respond to disinformation (Ibid:4). The Russian disinformation tactic is presented to be intelligent and advanced, with the report saying that Russia is "opting for smaller-scale, localised operations that are harder to detect and expose", and the action plan saying that Russia's campaigns are "systematic, well-resourced and on a different scale to other countries", giving a more detailed explanation of Russian's capabilities than the documents in period one (EEAS & European Commission 2019:3; EEAS & European Commission 2018:4). The Action Plan also states that other state-actors have adopted the strategies of Russia, saying that "other third countries also deploy disinformation strategies, quickly learning from the methods of the Russian Federation" (EEAS & European Commission 2018:4). Thus, new actors taking after Russia is also a new problem representation in period two.

5.2.2 What Presuppositions or Assumptions Underlie this Representation of the Problem?

The binary relationship between the EU and Russia is more strongly identified in the Action Plan and the report than the "Joint Framework on Hybrid Threats" in 2016. While the framework of 2016 did not mention Russia by name, the documents in period two call Russia out directly, even calling the Federation their biggest threat when it comes to disinformation and expressing worry that other actors are adapting their advanced disinformation tactics (EEAS & European Commission 2018:4). The emphasis on Russia as the biggest threat and Russia being the only actor mentioned by name implies that the EEAS continues to consider the Federation their biggest concern, increasing the "us vs. them" narrative concerning EU vs Russia. The new problem representation concerning new actors adapting Russia's disinformation strategy broadens this narrative. The EEAS, by connecting the other actors to Russia, further implies that the actors are against the EU, further emphasizing the "us vs. them" relationship.

The key concept cooperation continues to be evident in the Action Plan and the report. There is a continued emphasis on the inclusion of Union institutions, member states, civil society, but also on partners such as NATO and the G7 (EEAS & European Commission 2018:1-2, 10; EEAS & European Commission 2019:5, 9). The Action Plan states that the EU will work closely with NATO by exchanging information regarding disinformation (EEAS & European Commission 2018:8). There is also an increased emphasis on the responsibility of the private sector, with the Action Plan and the report highlighting the responsibility that online platforms have in countering disinformation. The special emphasis on online platforms highlights the restrained power the EU has over limiting Russian disinformation, as the private companies have control over what is published on their platforms.

Another key concept that is recognized in the Action Plan and the report is democracy**.** Democracy is discussed as being a core and proud value of the EU, with the report stating that "European democracy is only as strong as the active participation of its citizens" and declaring that the voter turnout was record high in the European Parliament elections of 2019 (EEAS & European Commission 2019:1). The Action Plan also emphasizes the democratic principle of freedom of expression, and the importance for its citizens to have access to information in order to create their own political stances (EEAS & European Commission 2018:1). Securing freedom of expression is a dilemma that democracies face when countering disinformation, since prohibiting disinformation spread on for instance social media could be considered to be against freedom of expression. This dilemma could be something that the policy is attempting to tackle by emphasizing the importance of democracy in the Union.

The categories are more specific when it comes to disinformation than the documents of 2015 and 2016. The EEAS and the Commission publishing an Action Plan and a report implies that the perception of the threat of disinformation has increased, as it is given more attention. In the Action Plan, Russia is mentioned the most under the subtitle "disinformation: understanding the threats and strengthening the European response", contributing to the notion that Russia is a big threat to the EU when it comes to disinformation (EEAS & European Commission 2018:3). Disinformation is also stated as being a part of "hybrid warfare", while the framework of 2016 referred to disinformation as "hybrid threat", reinforcing the discourse around disinformation as a legitimate and dangerous tactic connected to war (ibid:3).

5.2.3 How has this Representation of the Problem Come About?

With the history of Crimea and the general rocky relationship between the EU and Russia in mind, there are several more events that occurred during this time period that could have contributed to the increased attention given to Russian disinformation and its threat to European democracy in the Action Plan and the Report. The Action Plan states that "disinformation produced and/or spread by Russian sources has been reported in the context of several elections and referenda in the EU" (EEAS & European Commission 2018:3). In the Brexit referendum of 2016 Russia held an official neutral stance, but the Russian state-controlled media outlet Russia Today published several articles pushing for the "leave" side, and thousands of internet bots connected to Russia were identified leading up to the election also promoting "leave" (Stengel 2019:235-236). Although the US is not part of the EU, the Russian disinformation campaigns during the US election of 2016 also created worldwide attention regarding the new Russian tactic (Hedling 2021:841). The increased global acknowledgment of Russian disinformation campaigns inside and outside of the EU may have given the EEAS more leverage to pinpoint Russia in the documents, which is a change from earlier documents where they were more cautious in mentioning Russia.

5.3 Time Period Three: 2020-2021

5.3.1 What is the Problem Represented to Be?

In the two documents published in 2020 and 2021 the problem representation has to do with the COVID-19 pandemic. In the joint communication *Tackling COVID-19 disinformation - Getting the facts right* (2020) published by the EEAS and the Commission, disinformation during the COVID-19 pandemic is referred to as an “infodemic”. They mean that actors are taking advantage of the pandemic as a way to spread conspiracies which could be dangerous to the health of citizens and the democracy of the EU (EEAS & European Commission 2020:1). In the EEAS report and the joint communication Russia continues to be presented as a threat to the EU. The report is filled with examples of Russian disinformation, several stated as being against the EU’s strategy against covid-19 and the communication stating that:

> *“[...] [Russia]have engaged in targeted influence operations and disinformation campaigns around COVID-19 in the EU, its neighbourhood and globally, seeking to undermine democratic debate and exacerbate social polarisation, and improve their own image in the covid 19 context”* (EEAS & European Commission 2020:3).

Both the report and the joint communication, however, also represent China as a new actor in spreading disinformation. Even though there are more examples of Russian disinformation campaigns in the report, the EEAS also provides several examples of Chinese disinformation targeted against the EU. In the EEAS report, the problem of Russian disinformation during the pandemic is represented to be that it is undermining the EU and its institutions while promoting their own strategies, as a way to improve their general image (EEAS 2021b:1). Social media is still presented as a problem, with the joint communication stating cooperation with social media platforms is key in countering disinformation. They also state that the pandemic has led to more social media use (because of quarantine), which can lead to more disinformation spread (EEAS & European Commission 2020:1).

5.3.2 What Presuppositions or Assumptions Underlie this Representation of the Problem?

There is still an identified binary relationship between Russia and the EU in the documents of 2020 and 2021, and the EEAS report makes this relationship very clear. In the report by the EEAS several detailed examples where Russian disinformation is said to undermine the EU in different ways are highlighted. For example, the EEAS report states how Russian media outlets have "accused the EMA and the EU in general of political bias against the Russian-made vaccine" among several other points (EEAS 2021b:3). This differs from the documents from time period one and two where, although Russian disinformation is mentioned in the context of events such as the MH17 crash and democratic elections, there are few detailed examples of what narratives the disinformation campaigns are spreading. There are also more actors that have entered the playing field. China is pointed out in both the joint communication and the EEAS report. The narrative has changed from "EU vs. Russia" to "EU vs. Russia and China". Both Russia and China are accused in the report of spreading disinformation that discredits the EU. The report, however, states that while Russia has promoted China in other policy areas, they do not seem to be cooperating when it comes to vaccine diplomacy. (EEAS 2021b:6). The emphasis on China as a new actor is an escalation from period two, where new actors are mentioned as a potential threat but are not clearly stated. The representation of Chinese disinformation shows a broadening of the disinformation threat is occurring, with more actors involved.

The subtitles under which Russian disinformation is categorized in the EEAS report contribute to the notion that Chinese disinformation also is a threat to the EU. While most of the report discusses Russian disinformation, Russia and China are mentioned in two of the same subtitles: "Russian and Chinese state-controlled media target Western vaccines" and "Russian and Chinese state-controlled media accuse the EU (the West) of politicising the vaccines" (EEAS

2021b:4-5). Placing the two actors under the same category further emphasizes that the binary relationship between the EU and Russia has expanded to also include China.

Two key concepts continue to be identified: democracy and cooperation. Democracy continues to be presented as a target of Russian disinformation. The EEAS and the Commission state that the EU needs an approach that is “in line with our democratic values”, and that “our common values and democratic institutions, including free expression and free and plural media” are important in their fight against Covid-19 disinformation (EEAS & European Commission 2020:1). The emphasis on democratic values may imply, yet again, that the EEAS is tackling disinformation in a democratic way, without risking that their actions may be understood as censorship. The concept of cooperation is seen throughout the whole Communication, with a special focus on online platforms, but also with civil society, EU institutions, member states and international organizations such as NATO (EEAS & European Commission 2020:7). The continued emphasis on the responsibility of private companies implies that they have the most power in prohibiting the spread of Russian disinformation, as they have the ability to flag certain posts and fact check (Ibid:8). There is also a stronger emphasis on educating the public, as the EEAS report is stated as an effort to share information on disinformation “with civil society, media and expert communities” (ibid:5). The choice to publish reports especially aimed toward the public suggests that the EEAS is advancing its counter strategies against disinformation.

“Infodemic” is a new key concept found in the joint communication of 2020 (EEAS & European Commission 2020:1). To frame disinformation as being on the same level as the pandemic illustrates the EU’s perception of disinformation. By this comparison, the EEAS implies that just like a virus, disinformation can also spread at a rapid pace. Using the word “infodemic” to describe the disinformation climate during Covid-19 also suggests that the disinformation flows have increased, setting it apart from different times where disinformation has spread. Given that a pandemic has a negative connotation, calling disinformation during the Covid-19 outbreak an “infodemic” also implies that disinformation is a threatening phenomenon. Thus, the word choice by the EEAS suggests that they perceive disinformation more as a threat than previously.

5.3.3 How has this Representation of the Problem Come About?

The EEAS has so far recognized a multiplicity of vulnerabilities when it comes to Russian disinformation campaigns, such as democratic elections and disasters (like MH17). With the Covid-19 pandemic, it is not surprising that the discourse concerning the issue of Russian disinformation became harsher, such as calling it an "infodemic" and publishing reports that call out Russian disinformation. Health topics also have had a history of being especially vulnerable to disinformation, such as the KGB's "operation INFEKTION" during the AIDS epidemic (Stengel 2019:140). With a new disease, fear arises. This causes individuals to search for answers, even when there are no answers to be found yet. Diseases therefore make individuals especially vulnerable to disinformation, as fear creates a need to fill out our information gap. With the rise of social media in combination with the pandemic, disinformation campaigns have escalated and spread globally (Hazelton 2021:94-96). The increased amount of people staying at home has led to more time spent on social media, resulting in information overflows (Hazelton 2021:101). During the Covid-19 pandemic, Russia has boosted its own strategies in tackling the virus, while, according to the EU trying to undermine the EU's. The pandemic may explain the continued emphasis on social media in the EEAS documents, as they may recognize that citizens may be even more vulnerable to Russian disinformation during a time of fear.

The new recognition of China as a disinformation actor is partly linked to China's political relationship with Russia. As the EEAS report states, China and Russia are often allies in policy areas (EEAS 2021b:6). China's disinformation campaigns during the Covid-19 pandemic have also said to mimic Russia's previous tactics (Bernard et al. 2021:2). The perception of China's targeted disinformation campaigns towards the EU during the pandemic confirms the prediction that the EEAS had in the Action Plan on Disinformation and the report on the Action Plan, where they stated a worry that other states would adapt the Russian disinformation tactics.

6 Discussion

There are several meaningful connections that can be drawn from the WPR analysis that suggests a change has occurred in the EU’s perception of Russian disinformation as a threat. By applying the theory of securitization to the analysis, a gradual securitization of Russian disinformation can be identified. In the three time periods from 2015-2021, a framing is recognized that changes with the times. As different events, such as a pandemic and elections, have occurred and shaped the political climate, the perception of the Russian disinformation threat has changed with it.

Throughout 2015-2021, Russian disinformation is consistently stated as a threat to the EU. In the first time period (2015-2016), the EEAS avoided naming Russia as a disinformation spreader. In the second time period (2017-2019), however, Russia is stated as the EU’s biggest threat, clearly identifying Russian disinformation as an existential security threat. This pattern is continued in the third time period (2020-2021), where the EEAS report publishes official evidence of Russian disinformation campaigns. A strong “us vs. them” relationship is presented, where Russia is constantly seen as being against the EU. The gradual emphasis of Russian disinformation as a threat shows that a securitization is occurring. Even though Russian disinformation was already recognized as a problem in the first time period, the emphasis on Russia as a problem in the latter time periods shows that the EEAS has taken further securitizing moves in framing Russian disinformation as a threat. However, Russia is not the only actor being securitized. The last period also shows China being represented as a threat to the EU, broadening the disinformation threat to include another actor. The EEAS report of 2021 further confirms that a securitization is occurring, as it is especially geared towards the public. Hence, the EEAS is attempting the last step in the securitization process, which is when the public accepts the threat as such.

Furthermore, the threat of Russian disinformation can be understood by the escalation of focus areas in the documents. All time periods emphasize the importance of cooperation in battling disinformation, but there is a gradual specification of the concept of cooperation, which includes more actors. Time period one repeats civil society and member states as important actors, while time periods two and three also include EU institutions, private companies and partners such as NATO and the G7. Starting a cooperation with NATO, given the history of the relationship between NATO and Russia, may be a way for the EEAS to show Russia where they stand on the disinformation issue. Russia sees NATO as a national security threat highly connected to the U.S, and by cooperating with NATO, the EEAS gives the implication that the EU is fighting against Russia on this issue. Expanding the amount of actors (including strategic ones like NATO) that the EEAS are willing to cooperate with could imply another securitizing move, where the EEAS is framing Russian disinformation as being multifaceted and being a joint threat.

The focus also becomes more specific during the different time periods. While period one's main focus is hybrid threats in general and only mentions disinformation briefly as a threat to society and individuals, period two frames the threat differently. In period two, the main focus is the threat that disinformation can pose to democracy, the EU's democracy in particular. In period three, while it still emphasizes disinformation's danger to democracy, the focus shifts to health. This gradual framing on the threat of disinformation can be explained through different political and global events throughout the time periods. The first period reflects the aftermath of the Russian annexation of Crimea in 2014, which resulted in increased tensions between the EU and Russia. With the annexation, the EU also started to recognize Russian disinformation campaigns that promoted the Russian narrative. In the second period, a connection can be seen between the EEAS' emphasis on democracy and the multiple elections held during the period. For example, the alleged Russian disinformation campaigns during the U.S presidential election of 2016 may have caused an increased worry for the European Parliament Elections of 2019. The EEAS recognized the threat disinformation could have on democracy, and therefore framed it as such. When the Covid-19 virus became a global pandemic, disinformation was framed as an "infodemic". The phrasing shows a further securitization move, this time concerning the increased vulnerability that disinformation has on individuals during the pandemic.

By studying how the problem representation came about in each period, a correlation can be seen between the political climate and the securitization of Russian disinformation. In the beginning, Russian disinformation was more vaguely framed, while the second and third period see a specification of the threat. The EEAS’ attention concerning Russian disinformation effects has increased, and is gradually being presented as a bigger threat, proving that a securitization is occurring. This shows a change in the EU’s perception of the threat, where Russian disinformation is gradually being seen as more advanced, more broad and therefore more dangerous, inspiring other actors to adapt their strategies, such as China.

7 Conclusion

The aim of this thesis was to study whether there had been a change in the European Union’s perception of Russian disinformation as a threat in their discourse since 2015 until 2021. By analyzing mainly EEAS documents from the time period, it is evident that a change within the discourse has occurred. A securitization of Russian disinformation as a threat to the EU has gradually taken place. While the first period represented a vaguer perception of Russian disinformation as a threat, the problem representation became more specific through the years. A correlation can be identified between different political events and issues that have occurred during 2015 and 2021 and the securitization as threat. As the EU faced other challenges, such as elections and a global pandemic, the threat of Russian disinformation was connected and addressed to handle Russian disinformation in these changing contexts. Thus, the EU’s perception of Russian disinformation changed by gradually adapting to different challenges and recognizing that Russian disinformation could pose a threat to all of these problem areas.

Throughout the time period, an expansion of the threat perception of disinformation can be identified. Russia is no longer the only threat, China has also stepped into the playing field in the disinformation game, adapting the tactics used by Russia. For further research, it would be meaningful to study the EU’s perception of other actors, such as China, as growing threat when it comes to disinformation. It is clear that, from Crimea to Covid, disinformation has rapidly become a concern for the EU. With new actors adapting Russian tactics and technology advancing, disinformation will most likely continue and increasingly be seen as a security threat.

8 References

Bacchi, Carol. (2009). *Analysing Policy: What's the problem represented to be?* Frenchs Forest: Pearson Australia.

Bentzen, Naja (2018). "Online disinformation and the EU's response". *At a Glance, European Parliamentary Research Service*, PE: 620.230.

Bernard, Rose, Gemma Bowsher, Richard Sullivan & Fawzia Gibson-Fall (2021). "Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare". *Mary Ann Liebert Inc*, 19(1), pp. 3-12.

Boghardt, Thomas (2009). "Soviet Bloc Intelligence and Its Aids Disinformation Campaign". *Studies in Intelligence,* 53(4), pp. 1-24.

Borell, Josep (2021). *Russia: Speech by High Representative/ Vice President Josep Borell at the EP Debate*. March 28th 2021, Brussels. Retrieved from: https://eeas.europa.eu/headquarters/headquarters-homepage/97446/russia-speech-high-representativevice-president-josep-borrell-ep-debate_en (Accessed: 2021/05/27).

Buzan, Barry, Ole Wæver & Jaap de Wilde (1998). *Security: A New Framework for Analysis.* Boulder: Rienner.

Doroszczyk, Justyna (2018). "Russian Active Measures in Psychological Warfare". *Polish Political Science Yearbook,* 47(3), pp. 521-534.

EEAS (2019a). *About the European External Action Service (EEAS)*. Retrieved from https://eeas.europa.eu/headquarters/headquarters-homepage/82/about-european-external-action-service-eeas_en (Accessed 2021/05/27).

EEAS (2019b). *Countering disinformation*. Retrieved from https://eeas.europa.eu/topics/countering-disinformation/59411/countering-disinformation_en (Accessed: 2021/05/27).

EEAS. (2021a). *The European Union and the Russian Federation*. Retrieved from https://eeas.europa.eu/headquarters/headquarters-homepage/35939/european-union-and-russian-federation_en (Accessed: 2021/05/27).

EEAS (2021b). *EEAS SPECIAL REPORT UPDATE: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic (UPDATE DECEMBER 2020 - APRIL 2021).* Retrieved from https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-december-2020-april-2021/ (Accessed: 2021/05/27).

EEAS & European Commission (2016). *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats. A European Union Response*. JOIN(2016) 18 final.

EEAS & European Commission (2018). *Joint Communication to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions. Action Plan Against Disinformation*. JOIN(2018) 36 final.

EEAS & European Commission (2019). *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Commitee of the Regions. Report on the Implementation of the Action Plan Against Disinformation*. JOIN(2019) 12 final.

EEAS & European Commission (2020). *Joint Communication to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions. Tackling COVID-19 disinformation - Getting the facts rights.* JOIN(2020) 8 final.

European Commission (2021). *Tackling online disinformation*. Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/online-disinformation (Accessed 2021/05/27).

European Council (2015). *European Council Conclusions, 19-20 March 2015*. EUCO 11/15. (2021a). *About*. Retrieved from: https://euvsdisinfo.eu/about/ (Accessed: 2021/05/27).

EuvsDisinfo (2021a). *About*. Retrieved from: https://euvsdisinfo.eu/reading-list/ (Accessed 2021/05/27).

EUvsDisinfo (2021b). *Studies and Reports*. Retrieved from: https://euvsdisinfo.eu/reading-list/ (Accessed: 2021/05/27).

Floyd, Rita (2013). "Analyst, theory and security: a new framework for understanding environmental security studies". In Floyd, Rita & Richard A. Matthew (eds.), *Environmental Security: Approaches and Issues*, pp. 21-35. New York: Routledge.

Halperin, Sandra & Oliver Heath (2017). *Political Research: Methods and Practical Skills.* Oxford: Oxford University Press.

Hazelton, Alice (2020). "Once Upon Covid-19". In Giusti, Serenai & Elisa Piras (eds.) *Democracy and Fake News. Information Manipulation and Post-Truth Politics*, pp. 92-103, London : Routledge.

Hedling, Elsa (2021). "Transforming practices of diplomacy: the European External Action Service and digital disinformation". *International Affairs*, 97(3), pp. 841-859.

Hughes, James. (2013). "Russia and the Secession of Kosovo: Power, Norms and the Failure of Multilateralism". *Europe-Asia Studies*, 65(5), pp. 992-1016.

Jørgensen, Marianne & Louise J. Phillips (2011). *Discourse Analysis as Theory and Method.* London: SAGE.

Kovalčíková, Nad'a & Ariane Tabatabai (2020). "Lessons earned and lessons learned: What should be done next to counter the COVID-19 infodemic?". *European View*, 20(2), pp. 154-163.

Magdin, Radu (2020). "Disinformation campaigns in the European Union: Lessons learned from the 2019 European Elections and 2020 Covid-19 infodemic in Romania". *Romanian Journal of European Affairs*, 20(2), pp. 49-61.

NATO (2021). *Relations with the European Union*. Retrieved from NATO: https://www.nato.int/cps/en/natohq/topics_49217.htm (Accessed: 2021/05/27).

Orenstein, Mitchell A. (2019). *The Lands in Between. Russia vs. the West and the New Politics of Hybrid War.* New York: Oxford University Press.

Shu, Kai Amrita Bhattacharjee, Faisal Alatawi, Tahora H. Nazer, Kaize Ding, Mansooreh Karami & Huan Liu (2020a). "Combating disinformation in a social media age". *WIREs Data Mining Knowl Discov*, 10(1385).

Shu, Kai, Suhang Wang, Dongwon Lee & Huan Liu (2020b). "Mining Disinformation and Fake News: Concepts, Methods, and Recent Advancements" in Kai, Suhang Wang, Dongwon Lee & Huan Liu (eds.) *Disinformation, Misinformation, and Fake News in Social Media: Emerging Research Challenges and Opportunities*, pp. 1-19. Cham: Springer.

Sjöstedt, Roxanna (2017). "Securitization Theory and Foreign Policy Analysis". *Oxford Research Encyclopedia of Politics*, pp. 1-16.

Stengel, Richard (2019). *Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It.* New York: Routledge.

Sukhankin, Sergey (2020). "Covid-19 as a Tool of Information Confrontation: Russia's Approach". *The School of Public Policy Publications*, 13(3), pp. 1-10.

Ördén, Hedvig. (2020). *Securing Judgement: Rethinking Security and Online Information*. PhD Dissertation, Stockholm University, Stockholm.