M.A. in Political Science
with a Concentration in European Union Policy Studies
James Madison University

Supranational or Compartmental: Applying the Question of European Union Identity to the Topic of Disinformation

Eric Myhre

Abstract

The proliferation of disinformation is not a new phenomenon. However, the increasingly interconnected nature of the global environment means that disinformation is more effective now than ever before. Western societies are simultaneously experiencing a growing political stratification and third-party intervention in their respective democratic processes and institutions. State actors have utilized social media, hybrid warfare tactics, and automated disinformation tools to exacerbate divisions in society. Therefore, it is crucial that such societies develop sufficient capabilities to proportionately counter third-party interventionism. This paper aims to examine the relative counter-disinformation measures taken by the European Union (EU) in order to draw comparisons to those measures taken by individual EU member states. Thus, we are applying the classic EU debate of supranationalism versus state sovereignty to the topic of disinformation. In doing so, we hope to assess whether a supranational, EU-based strategy is more effective than a compartmental, member state-based strategy to counter disinformation. We first examine the body of EU action, followed by an examination of Baltic, Swedish, and German actions with the hope of ascertaining which pathway facilitates a more effective response.

Written for Topics in Foreign Policy and Internal Security (Mr. Iakovos Iakovidis).
Presented at the James Madison University – Max Weber Programme Graduate Symposium,
EUI, Fiesole, Italy, 12 April 2019.

Introduction

The proliferation of disinformation across Western democracies in the last decade has grown at an exponential rate. This disinformation is aimed at undermining the legitimacy and public trust in the institutions that these democracies rely upon. Thus, it is imperative that governments identify feasible strategies to defend against disinformation. This paper will be aimed at examining the relative merits of a supranational (European Union) approach to countering disinformation when compared to an individualized (member state) approach. The purpose then, will be to highlight advantages and disadvantages in said approaches, in order to ascertain where governments might best dedicate available resources. It is likely that a combination of these approaches is the most effective method of response. However, for the purposes of this analysis, a comparative lens will be utilized to highlight disparities in methods employed by the EU and its member states.

I contend that the comparison between an EU, supranational approach and an individualized, member state approach will show that there is a greater level of effectiveness in the latter. This is due to several factors. First, a geographic disparity in the threat of disinformation, along with its prevalence, produces a higher level of necessary response for some states more so than others. Second, the fact that disinformation is typically tailored to specific contexts means that it must be addressed with equally tailored strategies. Third and lastly, the breadth of the types of disinformation (social media, mass media, etc.) make the EU, as currently constituted, an inefficient actor for instituting practical countermeasures. Thus, I will argue that the EU is more effective when playing the role of facilitator in empowering member state capabilities.

In drawing this comparison, this paper will first provide background aimed at defining disinformation. Said background will provide an explanation of common modes or tactics in employing disinformation. Following this, I will then address the types of actors who have employed these tactics and how such tactics have evolved with the onset of the digital age. This analysis will then seek to compare the EU approach with those approaches employed by its constituent member states, based on regional and national configurations. In doing so, I will focus on three cases: the Baltics (Estonia, Latvia, and Lithuania), Sweden, and Germany. The majority of this analysis will focus on approaches meant to either identify or counter disinformation originating from the Russian Federation. Finally, this study will enumerate its findings and draw conclusions based on the cases examined.

Literature Review

Perhaps the greatest irony in the age of the internet "is that there is more information available at our fingertips than anytime in human history, but less and less confidence in that information" (Klurfeld and Schneider 2014, 3). This is the dilemma that is presented to the 21st century citizen, many of whom are reliant upon the internet in some manner of speaking. The proliferation and deployment of disinformation has become a growing area of concern in both national and international contexts. However, disinformation is not a new phenomenon. Whereas common citizens have become increasingly aware of its prevalence relatively recently, sovereign bodies have recognized and utilized disinformation for decades, if not centuries. Indeed, there is a fairly large body of scholarly literature committed to studying and analyzing it. This paper seeks to contribute to this literature by employing an evaluative analysis of the ways in which varying levels of EU governments respond to disinformation.

Defining Disinformation

In order to evaluate relative effectiveness in the ability to counter disinformation, it is important to first define what is meant when this word is used. As the larger public sphere has experienced a growing exposure or proximity to the knowledge of "disinformation", the word has become increasingly bandied about. A higher level of citizen recognition and understanding of tactics is largely a good thing. However, using the word disinformation becomes dangerous when used interchangeably with words of different meaning or when something entirely else is meant. This creates a watering-down effect, diminishing the perception or reaction to examples of disinformation which would otherwise be suitably visceral.

Disinformation, then, is "the distribution, assertion, or dissemination of false, mistaken, or misleading information in an intentional, deliberate, or purposeful effort to mislead, deceive, or confuse" (Fetzer 2004, 231). Thus, it can be described as an active measure which is meant to sway public perception toward or away from a particular stance, political or otherwise. The operative factor that defines disinformation is intent. While factually incorrect news and information does get disseminated to the public, it is not always done with sinister intentionality. Purveyors of disinformation intentionally employ notions or data that they know to be false, with the hope that such notions will be accepted as truth. Naturally, this means that it is put forth by an actor who has an interest in pursuing an agenda that would not otherwise be organically adhered to. Furthermore, it should be noted that there is often a misinterpretation of what is meant to be opinion, but which is consumed as fact. The primary agent in this case is the recipient rather than the source, exemplifying the fact that those who consume information have a responsibility to mitigate such consumption with a discerning eye.

An important distinction, then, should be made between disinformation and what is actually known as misinformation. Misinformation is typically “false information disseminated without an agenda by those who are either unfamiliar with the evidence or cognitively impaired” (Fetzer 2004, 238). Whereas disinformation implies the intentionality to mislead, misinformation arises out of an ignorance on the part of those producing it. While this ignorance should also be perceived as unacceptable, it is not as nefarious as tools meant to purposefully affect change based on their own falsehood. Another distinction should be drawn between disinformation and what has become known as “fake news”. This term has recently exploded in popularity and become something of a buzz word, particularly in the U.S. However, fake news is not necessarily disinformation. Fake news can define any information that is factually incorrect, intentionality aside. Therefore, fake news can be either disinformation or misinformation, though it is often interpreted as the former.

If it were to be used properly, it might represent a viable strategy for the identification of disinformation. Conversely, it can also be used to delegitimize factual information that does not agree with the stance put forth by an individual. Donald Trump has brought this term onto the forefront of political jargon, evoking its use even when there is credibility in a story that paints him in a negative light. This serves to blur and confuse the perception of reliable news, especially given Trump’s prominent position. Furthermore, it may polarize groups of people already distrustful of news not adhering to their beliefs (Guess, Nyhan, and Reifler 2018).This allows them to denounce as a lie anything that does not confirm their bias, even if it is legitimate or factual.

Disinformation Modes and Targets

There are varying modes or types of disinformation that can be utilized by an actor with a particular agenda. Modes can range from publishing falsified news stories to individual comments on social media platforms. Fetzer (2004) put forth six levels of disinformation that are commonly used by an array of actors, including news media, scholars, critics, etc. Aside from disseminating outright falsehoods, disinformation can also be characterized by things like intentional omission, with the purpose of presenting something as different than what it is. This often happens when someone reviews or responds to previously posited arguments with the intention to empirically disprove, while ignoring the most important evidence that the conclusions rely upon.

Another mode of disinformation might be described as one that climbs the ladder of legitimacy. This can occur when an agent with an agenda provides a receiving party, who is usually perceived as legitimate, with information that the original agent knows to be false. The receiving party is usually one that will not be rationally connected to the original agent, providing feasible deniability. The receiving party will then disseminate said information, often without the knowledge of its falsehood. Other publishers or individuals will subsequently pick up and spread the information, through word of mouth or publishing, creating an exponential growth of the original fabrication. If somewhat believable, the disinformation can grow to be put forth by mass media, which further legitimizes its credibility. Eventually, it may spread to an extent that makes it nearly impossible to completely negate. Even with the provision of evidence and explanations which prove that it is indeed disinformation, there is no guarantee that this evidence will be consumed by those who have bought-in to the notion. An example of this process is seen in the assertion that the U.S. manufactured the HIV/AIDS virus in a governmental lab (Romerstein 2001). Another is that President John F. Kennedy was assassinated by the CIA. These falsehoods are still believed by a number of individuals to this day.

The targets of disinformation, as with its modes and tactics, are varied. These targets can be individuals, demographic groups, political parties, and even entire societies. Individuals, such as politicians or public figures, are often targeted if they are perceived to represent credible opposition to the agenda of those producing the disinformation. It is likely that such individuals are able to refute false claims, though not without lasting damage to their reputation. Even if the individual is able to disprove fabricated assertions, the disinformation will influence previously held dispositions toward said individual. This can be especially consequential if the target is, for example, a politician in a highly contested political election in which the margin for victory is decidedly slim.

The most common targets of disinformation campaigns are typically the common citizens in a given demographic group, society, or nation-state. This is particularly true of democratic systems, in which the populace holds the power of political determination. If disinformation efforts with the intent of catalyzing public action can create a false perception, it may undermine the legitimacy of established media or governmental institutions. Many citizens are not inclined to fact check information coming from what they perceive as a credible source, which in actuality is not. Such efforts can be particularly potent when consumed by citizens with lower levels of education and higher political stratification. These groups are simultaneously unlikely to perceive the disinformation as false and more likely to operationalize it by voting in elections. This is also true concerning disinformation efforts focused toward political parties. In the U.S., for example, the existing partisan divide between the left and right is highly discernable. Thus, disinformation that denigrates one party has a fair chance of being accepted by the other, given the relative disdain between the two. This serves to deepen political, and thus personal, divides between fellow citizens, resulting in a more fragmented and unstable social sphere (Asmolov 2018).

Disinformation in the 21st Century

While disinformation has subsisted throughout various societies and eras, it is perhaps more dangerous now than ever before. This is due to the increasingly interconnected nature of the world brought on by the digital age. The exponential growth of technological capabilities has provided innumerable benefits to citizens’ quality of life and economic prospects. However, it has also exposed the danger present in a world where information can be published and consumed without a formal vetting process. Traditional media outlets (newspapers, radio, television, etc.) have sought to maintain the factual integrity of their product in order to ensure a level of trust from consumers. Furthermore, most of this traditional media adheres to a code of ethics which enhances legitimacy. For decades, society consumed this type of media due to the limited range of choices present to them. This has changed with the onset of the internet age, where anyone with a keyboard and connectivity capability can disseminate information at will.

The proliferation of technology has extended into nearly every aspect of daily life, including basic human interaction. This is manifested in the popularity of social media, where a growing number of individuals now consume a majority of their information. Naturally, this presents a ripe opportunity for those pursuing an agenda through disinformation. As the world's technological capability has evolved, so too have disinformation tactics seeking to take advantage of previously unreachable targets. Both state and non-state actors (political extremists, hate groups, etc.) have utilized these fora to operationalize disinformation strategies, which effectively avoid the fact-checking or vetting process in traditional media. Social media platforms (Facebook, Twitter, Instagram, etc.) present an opportunity for disinformation to take on a life of its own after being disseminated. This occurs through individual exposure to false or intentionally misleading sources of information, "which are then circulated through personal networks" (Warwick and Lewis 2017, 26). Those who experience this sharing might subsequently circulate the sources through their own networks, beginning the process anew.

Another factor that improves the ease with which disinformation is disseminated through social media is the use of what are referred to as 'bots'. Essentially, bots are an aspect of what is known as "computational propaganda – the use of algorithms, automation, and human curation to purposefully distribute false or misleading information over social media networks" (Tucker, et al. 2018, 23). These are fake accounts that utilize programmed patterns of action to create online posts. These bots can post much faster and along a wider swathe of topics than human users are capable of in the same amount of time. The resources at the disposal of state producers of disinformation gives them the ability to deploy thousands of such bots at any given time. When masses of these algorithm-based accounts are used by state actors, they can persuade or provoke entire segments of society. A disinformation tactic closely related to using bots is the use of what are known as 'trolls'. Trolls are employed in much the same way as bots: using fake accounts to post intentionally misleading information under false pretenses. The use of bots and trolls will be expanded upon when addressing particular cases of state-backed disinformation.

One of the most concerning aspects in the deployment of technology for disinformation has been the ability to distort perceptions or reality. The increase in the complexity of programming and algorithm-based splicing has resulted in an ability to create things that lie beyond a human's ability to discern their legitimacy. An example of this is what are known as "deep fakes". Deep fakes utilize competing algorithms in which one tries to create an image that the other cannot discern from real images, while the other tries to identify the manufactured image. This allows the algorithm to rapidly engage in self-learning, progressively creating more and more realistic images or audio. In practice, these algorithms can be used to create videos or audio clips of individuals doing or saying things that they had no actual part in. This represents a clear and present danger to the legitimacy of democratic processes by undermining citizens' ability to trust officials and institutions. Particularly concerning is the potential ease with which these capabilities might spread. Despite their relatively recent development, "commercial and even free deep fake services have already appeared in the open market, and versions with alarmingly few safeguards are likely to emerge on the black market" (Chesney and Citron 2019, 148). Specifically, the weaponization of deep fakes by state actors like Russia would be a potent threat to Western political institutions.

Objectives and Methodology

This paper seeks to observe and evaluate the relative merits between an individualized, member state approach and a supranational, EU-level approach to discerning and countering disinformation. For the purposes of this evaluation, I will focus mainly on those approaches aimed at countering disinformation identified as originating from the Russian Federation. In doing so, I will first observe the manner in which the EU has committed to addressing disinformation. This will include a discussion of established task forces, along with their delegated roles and sphere of action. I will then observe countermeasures taken by member states in addressing disinformation. This will be state-specific, noting disparate governmental mandates, agencies, and public efforts. I will lend consideration toward the confines of regional contexts and the disproportionate perceptions of threat therein. Member states from differing EU regions will be examined in order to assess patterns across the EU. Much of the discussion will focus on eastern and northern EU member states, given their proximity to the Russian Federation and the presence of ethnically Russian demographics as parts of their population.

EU Approaches to Disinformation

The EU's coordinated response to the rising prevalence of disinformation has been discernable, though perhaps insufficient in substance. There have been a number of Parliamentary resolutions addressing this subject that have been passed, along with the establishment of a task force meant to counter disinformation. Furthermore, EU legislative action like the General Data Protection Regulation have focused on protecting privacy and citizen data. While these are steps in the right direction, they seem to be more reactive than proactive, aimed at precluding criticism for not having addressed this danger. The enacted measures have proven useful in a variety of ways, though they have failed to produce substantive change or comprehensive deterrence of disinformation.

Perhaps the most effective action that has been taken toward countering disinformation at the EU level is the establishment of the East Stratcom Task Force, operating under the purview of the European External Action Service (EEAS). The task force was established in 2015, with the aim of identifying, collating, and disseminating examples of disinformation in varying languages. It is manned by a combination of "seconded staff and a network of volunteers" (Bassot 2018). The bulk of the work done by this task force is manifested as a weekly publication that analyzes the content of individual cases. This publication is called the *Disinformation Review*, accessible via newsletter and their website EUvsDisinfo, and purports to be "the only publicly accessible, international database of disinformation cases" (East Stratcom Taskforce 2018). The *Disinformation Review* is mainly concerned with what is identified as "pro-Kremlin" instances of disinformation, meaning those cases that aim to further a Russian agenda. The *Disinformation Review* identifies the source of disinformation cases, though they include a disclaimer noting that these sources are not necessarily formally aligned with Russia. According to their website, the EUvsDisinfo has identified over 5,100 cases of disinformation as of Spring 2019.

While effective, and indeed necessary, it is worth considering whether the East Stratcom Task Force has realized its full potential. Its composition as a group of repurposed employees and volunteers implies that its importance has been underemphasized. The EU might be better served by expanding its operational expertise and employing staff specifically dedicated to this area. However, there have been efforts to improve the task force through Parliamentary requests and communications. Specifically, a resolution in 2016 aimed at this improvement “by turning it into a fully fledged unit within the EEAS…with proper staffing and adequate budgetary resources” (European Parliament 2016). Furthermore, the EU significantly expanded the budgetary emphasis placed on countering disinformation through a 1.1-million-euro pilot program called the StratCom Plus project. This project would reinforce the East StratCom Task Force in order to “increase EU capacity on fact-checking disinformation in and beyond the EU, by boosting the skills of staff” (Committee on Budgets 2017, 33). This expansion in capability and resources has been important in improving the task force’s ability to perform its role. However, its progress and achievements might have been greatly increased had these measures been dedicated from the onset. Moreover, it is unlikely that the EU has even come close to something of a proportional response to the Kremlin’s disinformation, given “the huge resources dedicated to propaganda activities by Russia” (European Parliament 2016).

In 2017, a European Parliament resolution called for the European Commission to take a more active role and “to analyze in depth the current situation and legal framework with regard to fake news, and to verify the possibility of legislative intervention to limit the dissemination and spreading of fake content” (European Parliament 2017). In answering this call, the European Commission established a “High-Level Expert Group representing academics, online platforms, news media and civil society organizations” (European Commission 2017). The conclusions of the High-Level Expert Group rested on five pillars or recommendations. These include enhancing transparency of online news, promoting media and information literacy, develop tools for empowering users and journalists to tackle disinformation, safeguard the diversity and sustainability of the European news media ecosystem, and promote continued research on the impact of disinformation in Europe (European Commission 2018).

More recently, the European Parliament adopted another resolution that urges for a greater dedication of resources to countering hybrid threats like disinformation. The resolution comes ahead of impending 2019 elections, emphasizing the threat that is faced by the democratic institutions of the EU. In addition to Russia, the resolution identifies China, Iran, and North Korea as perpetrators of the continued interference. The proposal also comes amidst a published study by “civil rights group Avaaz, that shines a light on the fact that fake news circulating during the French Yellow Vest movement reached over 105 million views on Facebook" (Brzozowski 2019).

Another avenue for the countering of disinformation has been seen in collaborative efforts between the EU and NATO. This was practically manifested in the establishment of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), headquartered in Helsinki in October 2017. Currently, 17 EU member states participate in the program, along with Norway, the U.S., and Canada. While the EU as a whole is not a participant, the Hybrid CoE remains open to any EU member state or NATO ally. Essentially, the Hybrid CoE's mission is to provide an educative role to participant states in order to identify vulnerabilities, increase resilience to disinformation, and improve member states' comprehensive judgement toward hybrid warfare (Hybrid CoE 2019).

European Parliament resolutions and European Commission reports have been invaluable in setting the tone for necessary steps in countering disinformation. The establishment of the East StratCom Task Force, High-Level Expert Group, and Hybrid CoE are examples of tangible efforts to improve hybrid and disinformation resilience. However, these efforts might be best described as facilitative. Other than the *Disinformation Review* published by the East StratCom Task Force, much of these efforts are aimed at educating or improving the capacities of subsequent member states. Even the *Disinformation Review* is a purely informational resource rather than one that counters disinformation, though it is likely useful in deterring more flagrant cases. Rather than directly combating disinformation on a wide scale, the EU has sought to equip its constituent parts with the necessary ammunition to do so themselves. This is in line with the proposition put forth at the beginning of this paper; that an individualized, or nationally tailored approach is best suited to countering disinformation.

Member State Approaches to Disinformation

While disinformation campaigns and instances are a threat to the democratic viability of the greater EU, this threat is manifested through a diverse compartmentalization of targets. The cases of disinformation and fake news are specialized for maximum impact in their deployed audience. The European Parliament itself has concluded that much of the disinformation levied against its constituent nations is employed in "different forms and uses various tools, often tailored to match EU Member States' profiles, with the goal of distorting truths, provoking doubt, [and] dividing Member States" (European Parliament 2016). Counter-disinformation strategies are also variable, depending on the member state. They can include media literacy education, monetary fines, or identifying and debunking disinformation cases. It is worth mentioning that member states are also likely to employ state-level strategies that are not accessible to the public.

The Russian Federation has been deft at maintaining plausible deniability in playing a formal role as the origin for many cases of disinformation. While there has been fairly incontrovertible evidence of Russian state-sponsored meddling (i.e. the Internet Research Agency), they have been able to assert an absence of illegality in their actions. Thus, one of the most effective methods at the disposal of member states in mitigating the spread of disinformation is to place the onus on the consumer, rather than the disseminator. This can be achieved through an increase in the public's level of internet and media literacy. Petranová, Hossová, and Velický (2017) show that some EU member states, such as Great Britain, Denmark, Finland, Sweden, Belgium, the Netherlands, Hungary, Germany, and Austria, already have an established tradition of providing education in media literacy. However, it is worth noting that this education is provided in varying forms and effectiveness, along with differing areas of emphasis (i.e. journalism, safety on the internet, technical skill, critical thinking, etc.). Of particular importance are existing initiatives that focus on "the development of abilities and skills related to critical thinking and media content analyses…to look critically at published information and avoid dangers of the Internet" (Petranová, Hossová, and Velický 2017, 62). Enhancing media literacy might seem to be an abstract or ambiguous goal in building resistance to disinformation. However, some cases have shown that it can have a practical impact on a societal level. Indeed, Finnish officials have asserted that increased public recognition of disinformation through media literacy has resulted in the closing of the Finnish arm of *Sputnik* as a result of diminished readership (Jopling 2018).

Conversely, member states like Latvia, Lithuania, Poland, and even France have an arguably insufficient level of media literacy provided through either formal or informal pathways. Interestingly enough, these are four of the member states which have seen extensive occurrences of Russian disinformation cases. Thus, it would likely behoove these states to take a more active role in this sphere by further incorporating its importance in educative and extracurricular programs. While the EU can establish independent programs to encourage the growth of media literacy, education is a member state competence. Ultimately, this means that it is up to individual countries to design and institute media literacy curricula, especially targeted toward the youth. Therefore, “it will require more than individual champions, it will require” (Klurfeld and Schneider 2014, 23) member state governmental actions to bring about such changes in these states.

The Baltics

The northeastern member states of the EU are those that have the greatest geographic proximity to Russia. Logically, this means that the Russian sphere of influence is more present in this region than in others. While the occurrence of Russian election meddling and disinformation dissemination has been relatively recent in the U.S., eastern EU member states have been dealing with this reality for years. One simply has to compare the defense spending of these member states (as percentage of GDP) with that of other, more western member states to discern the higher level of perceived threat caused by Russia. This is reinforced by greater levels of commitment from Poland and the Baltics (taking into consideration the relativity in available state resources) to NATO.

The Baltics at once lack the disposable resources of more wealthy or populated EU member states while debatably experiencing a proportionately greater exertion of Russian influence. Being former organs of the Soviet Union, Estonia, Latvia, and Lithuania all have large ethnically Russian demographics. This makes Russian-sourced disinformation and hybrid tactics particularly effective within Baltic borders. Examples of such tactics are varied in nature, including the proliferation of Russian state-sponsored media and publications (television, print, online, etc.), the use of bots and trolls on social media platforms, and instances of infrastructural sabotage.

Pro-Kremlin media content within the Baltic countries is often aimed at Russian demographics by portraying the Russian Federation in a highly favorable light. This can include false information regarding Russian actions in Ukraine, disinformation portraying the West as unsavory or corrupt, and appeals concerning the democratic legitimacy of Russian politics. Investigations into varying Baltic media outlets have discovered that several are owned or controlled by pro-Kremlin actors. The news portal *Baltnews*, which operates in all three Baltic states, purports to be locally sourced and operated. However, a series of documents have uncovered that it is linked to the Russian multimedia conglomerate *Rossiya Segodnya* through a series of holding companies and varying owners (Spriņģe and Jemberga 2017). Another media outlet from Latvia, called the First Baltic Channel, often rebroadcasts Russian state programming and is reported to be tied with pro-Moscow politicians (Sarlo 2017). Outlets such as these provide platforms for pro-Kremlin or anti-Western sentiments to be put forth while operating under the guise of impartial journalism. Another example of media interference occurred in April 2017, when the Lithuania arm of the Baltic News Service in Vilnius was hacked and subsequently produced a false story asserting that US troops had been poisoned by mustard gas in Latvia (Gerdziunas 2017).

The Baltics have taken a fairly direct approach in countering interference in the media, constituted largely through fines and suspensions. Latvia fined the First Baltic Channel twice in 2014 and once in 2015, along with a separate radio station, for disseminating fake content from Russian news sources. In 2014, Latvia also suspended RTR Planeta (a Russian TV station) for three months after allegedly provoking an “incitement to war or the initiation of a military conflict” (EER News 2014). Lithuania has taken a similar line, suspending the First Baltic Channel for publishing false information concerning a historical event. Furthermore, the Baltics have worked to offer news outlets in the Russian language to grant an impartial alternative for the Russian-speaking demographics in their countries. Latvia has facilitated the work of the independent Russian publication *Meduza*, while Estonia committed to broadcasting its own Russian-language channel, ETV+ (Sarlo 2017). Meanwhile, Lithuania utilizes the U.S.-funded Radio Liberty, which broadcasts credible news and information in Russian and Belarusian languages (Jopling 2018).

The Baltics also strive for multilateral cooperation with NATO and its allies in advancing defensive capabilities against disinformation and hybrid threats. Two examples of this cooperation are the NATO Strategic Communications Centre of Excellence (StratCom COE) in Riga, Latvia and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. Both centers conduct research addressing digital threats, while CCDCOE also executes training programs and cooperative exercises to increase member capabilities. In 2016, StratCom COE produced a report detailing the use of state-backed trolls within Latvia. It found that pro-Russian trolling was evident in the Latvian online space, though to a lesser extent than expected. However, the content was often anti-U.S. in nature and was found to be “a small but important part of a larger machinery aimed at influencing the public in NATO member and partner countries” (NATO 2016, 81). In countering this occurrence, the report outlined ways for online users to identify which accounts or comments were likely troll-related. Furthermore, the reports detailed methods that might be utilized by Latvian mass media and government institutions to mitigate the spread of disinformation and trolled content.

The Baltics have also been effective in mobilizing their populace through a grassroots level approach. Citizens in Baltic countries have taken it upon themselves to individually counter the efforts of Russian disinformation. Playing off the name trolls, these citizens are known as ‘elves’. Ranging from academics to students, this movement is constituted by thousands of individuals, who “expose and combat false claims and contested narratives as fast as possible” (Peel 2019). The elves can fulfill several roles, from disproving cases of fake news to identifying individual troll accounts. These individuals are an invaluable tool for the Baltic states, in that they do not require an allocation of government resources and work to spread public awareness from the ground up.

Sweden

Similar to the Baltic states of Estonia, Latvia and Lithuania, the Scandinavian region has also been subject to potent disinformation efforts from Russian sources. In particular, Sweden has recently been a frequent target for Russian operations. Cases of fake news and false publications have been reported across several levels of Swedish media. The Swedish arm of Sputnik has been an active agent in the country’s media landscape, notably emphasizing anti-Western sentiments and stories. Sweden has also seen the proliferation of forged documents which take the form of communications from official or public figures. These forgeries have been well-crafted, appearing as perfectly legitimate to the undiscerning eye. At least one of these forgeries seems to have made its way into the mainstream media of Sweden, exemplifying its ability to mislead even professional journalists, let alone the average online user (Kragh and Åsberg 2017).

As with the country's traditional media sources, the Swedish social media environment has not been spared from coordinated disinformation. The use of automated bots and troll accounts have been utilized to sow division among the native population along lines of ideology and political predisposition. The Kremlin's social media efforts have been aimed at a number of topics. For example, political tensions have been further exacerbated by playing on party divides present in the citizenry. Another target for inflammatory content has been the growing racial resentment that has arisen as a product of extensive immigration. However, the largest focus of disinformation in Swedish social media interactions has been NATO. This is perhaps Russia's foremost priority in Sweden, manifested as a "security order [aimed at] minimizing NATO presence in the region" (Kragh and Åsberg 2017, 808). The goal of this social media engagement is to undermine public support for any prospective NATO-Sweden cooperation.

Sweden has taken several approaches to countering the disinformation that has been tailored toward their people and institutions. One of these approaches is to emphasize education on media literacy to better equip consumers of information. Sweden has taken the initiative of launching "programmes to teach children to differentiate between real and fake sources as early as primary school" (Jopling 2018, 13). The *Swedish Media Council* is active in teaching greater media literacy to parents, with the hope that they will subsequently provide their children with the tools to recognize illegitimate information. Another program is *Media Compass*, which focuses on ensuring that students have the skills necessary to critically analyze newspaper content (Petranová, Hossová, and Velický 2017).

Prominent Swedish news companies and governmental agencies have also contributed in improving the health of their informational sphere. Several of the leading domestic media outlets have banded together to digitally confront false stories (Löfgren 2017). The Swedish Civil Contingencies Agency, created in 2009, has been tasked with identifying potential vulnerabilities to coordinated disinformation that may exist in governmental institutions. This involved working with the Swedish Election Authority and police agencies to ascertain the government's ability to withstand foreign influence. The country's political parties took steps in enhancing the security of email servers and systems to ward against influence in campaign and election operations (Jopling 2018). Additionally, the Swedish Security Service has been working to debunk the content in forged documents and prevent further circulation (Lanoszka 2016). In setting the defense priorities for 2016-2020, the government took steps to reinforce the capabilities of the

Swedish Defense Intelligence Authorities and set forth prospects for the creation of a new agency to counter disinformation. This agency would focus on creating a “psychological defense [seeking] to maintain…open and democratic society with freedom of expression” (Swedish Ministry of Defense 2015).

Germany

The scope of Russian-sourced disinformation has not been exclusively limited to the member states located on the fringes of the EU. Germany, a member state in the heart of the EU, has also been subjected to third-party influence campaigns and hybrid tactics. In addition to geographic differences between the aforementioned states, Germany also represents a different case in terms of economic and governmental resources. The health of their economy and relative efficiency of government means that the Germans are more suitably equipped to handle foreign influence. Moreover, Germany represents a substantial market for Russia’s exports of fuel and energy resources. It might be argued that this works to mitigate the Russian emphasis on disinformation efforts in Germany due to a desire to preserve market access. In other words, the Russians likely know on which side their bread is buttered, as it were.

However, this does not mean that foreign influence efforts have not targeted Germany. Russia has allegedly carried out cyber attacks on both the German Parliament and German Foreign Ministry in recent years. Furthermore, the German Federal Office for Information Security has also accused Russia of perpetrating coordinated attacks against German energy providers (Jopling 2018). In addition to these attacks, Russia has worked to craft disinformation cases targeting the German public. A prominent example of this is what has been referred to as the Lisa Case. In 2016, a 13-year-old girl in Germany went missing for over 24 hours. Subsequently, Russian media outlets reported that she had been raped by migrants, which turned out to be false. However, individuals and right-wing groups spread the information on German social media, causing an inflammatory mobilization that eventually made its way into the mainstream media (Meister 2016).

In responding to such tactics, the Germans have taken several measures. Similar to Sweden, Germany utilized its intelligence services to identify and shore up network vulnerabilities preceding the 2017 elections. Most notably, the head of Germany’s domestic intelligence agency directly expressed the dangers of Russian disinformation tactics to the German public (Jopling 2018). This represents a break from other intelligence services, who typically rely on more clandestine methods of countering foreign influence.

Another mechanism for preventing disinformation might be described as rhetorical deterrence. German officials from varying levels of government issued direct statements detailing the prospects for proportionate responses should there be evidence of Russian disinformation meddling. Whereas other nations have not issued such statements or were subject to interference prior to it becoming common knowledge, Germany made clear that they would not stand for external influence in internal affairs. Examples include a meeting of the Federal Security Council which explicitly discussed mechanisms for retaliation, a reportedly direct Chancellery message, and statements from prominent politicians, civil servants, and intelligence officials (Brattberg and Maurer 2018). As with the importance of the German-Russian energy relationship, it is feasible that Moscow considered political relations with Berlin as too valuable to risk over disinformation campaigns during elections.

Perhaps the most effective German mechanism for countering fake news and disinformation is the decision to hold social media platforms responsible for policing their own spheres. In 2017, Germany instituted the Network Enforcement Act to spur social media companies to take a janitorial role toward false or harmful content. The act requires such companies to provide accessible avenues for users to report false or illegal content, while removing such content within 24 hours if it is indeed found to be false or illegal. If the companies fail to remove this content, they can be subject to fines of up to 50 million euros. Furthermore, the act requires social media platforms to submit reports of disinformation management twice per year (German Federal Ministry of Justice and Consumer Protection 2017).

Conclusion

The proliferation of disinformation, from both state and non-state actors, is unlikely to diminish in the near future. Rather, it is likely to increase given its relative effectiveness. Thus, it is advantageous to ascertain the most efficient way to combat disinformation. This paper aimed at observing differing approaches to disinformation from a member state level versus a supranational level. In doing so, I examined efforts and measures taken by varying EU institutions. I also examined differing member state approaches seen in the Baltics, Sweden, and Germany.

Evaluating the relative merits of the EU as a system of governance can be quite difficult. Its construction as a *sui generis* body can be both a boon and an obstacle. Through this analysis, I have found that the member state approach has allowed for greater expediency of action and the possibility for proportionate response. The preservation of sovereignty found in many member states allows for the unitary nature that is often required when countering disinformation. In the same manner, the preservation of national identity is useful in mobilizing a coordinated public response to falsified information. Member states are also more readily able to articulate relevant dangers to their population, as many EU citizens remain out of touch with Brussels. As exemplified in the member states addressed, an individualized or tailored approach is often required to counter disinformation that is equally tailored.

The supranational approach to disinformation is useful, though perhaps inadequate in meeting the scale of this problem. In particular, the EU is less capable of finding consensus from its constituent parts than centralized systems like the U.S. or Russia. Furthermore, the EU's budget and resources at the supranational level are decidedly marginal when compared to centralized powers. Thus, the EU is best served in performing the role that it has already assumed. That role being a facilitator and educator for the member states that it answers to. The EU's past approaches to countering disinformation can largely be described as calls to action and a setting of priorities. While these roles are valuable, they are only operationally effective when actualized by member state responses.

References

Asmolov, Gregory. 2018. "The Disconnective Power of Disinformation Campaigns." *Journal of International Affairs* 71, no. 1.5: 69-76.

Bassot, Etienne. January 2018. "Ten Issues to Watch in 2018." *European Parliamentary Research Service.*

Brattberg, Erik, and Tim Maurer. May 23, 2018. "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks." *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

Brzozowski, Alexandra. March 14, 2019. "Parliament Calls for EU Measures to Counter Hostile Disinformation Campaigns." *Euractiv*. https://www.euractiv.com/section/digital/news/parliament-calls-for-eu-measures-to-counter-hostile-disinformation-campaigns/.

Chesney, Robert, and Danielle Citron. February 2019. "Deepfakes and The New Disinformation War: The Coming Age of Post-Truth Geopolitics." *Foreign Affairs* 98.

East Stratcom Taskforce. "About - EU vs Disinfo." Accessed March 18, 2019. https://euvsdisinfo.eu/about/.

ERR Staff. April 7, 2014. "Concerns About Propaganda Media Sites Spread Beyond Baltics." *ERR News (Estonian Public Broadcasting).* https://news.err.ee/112182/concerns-about-propaganda-media-sites-spread-beyond-baltics.

European Commission. March 12, 2018. "Final Report of the High Level Expert Group on Fake News and Online Disinformation." https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

European Commission. November 13, 2017. "Next Steps Against Fake News: Commission Sets Up High-Level Expert Group and Launches Public Consultation." http://europa.eu/rapid/press-release_IP-17-4481_en.htm.

European Parliament. June 15, 2017. "Online Platforms and the Digital Single Market." http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0272+0+DOC+PDF+V0//EN.

European Parliament. November 23, 2016. "EU Strategic Communication to Counteract Anti-EU Propaganda by Third Parties." http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0441&format=XML&language=EN.

European Union External Action Service. November 2015. "EU East StratCom Task Force." http://www.tepsa.eu/wp-content/uploads/2015/12/Kimber.pdf.

Fetzer, James H. May 2004. "Disinformation: The Use of False Information." *Minds and Machines* 14, no. 2: 231-40.

Gerdziunas, Benas. October 8, 2017. "Baltics Battle Russia in Online Disinformation War." *Deutsche Welle*. https://www.dw.com/en/baltics-battle-russia-in-online-disinformation-war/a-40828834.

German Federal Ministry of Justice and Consumer Protection. 2017. "Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act, NetzDG) -

Basic Information." https://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html.

Guess, Andrew, Brendan Nyhan, and Jason Reifler. January 9, 2018. "Selective Exposure to Misinformation: Evidence from the Consumption of Fake News During the 2016 U.S. Presidential Campaign." *European Research Council*. http://www.ask-force.org/web/Fundamentalists/Guess-Selective-Exposure-to-Misinformation-Evidence-Presidential-Campaign-2018.pdf.

Jopling, Lord. October 1, 2018. "Countering Russia's Hybrid Threats: An Update." *NATO Parliamentary Assembly - Committee on the Civil Dimension of Security*. https://www.nato-pa.int/download -file?filename=sites/default/files/2018-12/166%20CDS%2018%20E%20fin%20-%20HYBRID%20THREATS%20-%20JOPLING_0.pdf.

Klurfeld, James, and Howard Schneider. June 2014. "News Literacy: Teaching the Internet Generation to Make Reliable Information Choices." *Center for Effective Public Management - The Brookings Institution*. https://www.brookings.edu/wp-content/uploads/2016/07/Klurfeld-Schneider_News-Literacy_June-2014.pdf.

Kragh, Martin, and Sebastian Åsberg. 2017. "Russia's Strategy for Influence Through Public Diplomacy and Active Measures: The Swedish Case." *Journal of Strategic Studies* 40, no. 6: 773-816.

Lanoszka, Alexander. 2016. "Western Intelligence and Counter-intelligence in a Time of Russian Disinformation." *Institute for European Studies*. http://openaccess.city.ac.uk/16239/1/LanoszkaIESPB.pdf.

Löfgren, Emma. November 7, 2017. "How Sweden's Getting Ready for the Election-Year Information War." *The Local*. https://www.thelocal.se/20171107/how-swedens-getting-ready-for-the-election-year-information-war.

Meister, Stefan. "The "Lisa Case": Germany as a Target of Russian Disinformation." *NATO Review Magazine*. https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm.

Muresan, Siegfried, and Richard Ashworth. October 2017. "2018 Budgetary Procedure." *Committee on Budgets*. http://www.europarl.europa.eu/cmsdata/129602/budg2018-doc6-txt-2-en.pdf.

NATO Strategic Communications Centre of Excellence. 2016. "Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia." https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0.

Peel, Michael. February 4, 2019. "Fake News: How Lithuania's 'Elves' Take on Russian Trolls." *Financial Times*. https://www.ft.com/content/b3701b12-2544-11e9-b329-c7e6ceb5ffdf.

Petranová, Dana, Monika Hossová, and Peter Velický. April 2017. "Current Development Trends of Media Literacy in European Union Countries." *Communication Today* 8: 52-64.

Romerstein, Herbert. 2001. "Disinformation as a KGB Weapon in the Cold War." *Journal of Intelligence History* 1, no. 1: 54-67.

Sarlo, Alexandra. July 6, 2017. "Fighting Disinformation in the Baltic States." *Foreign Policy Research Institute*. https://www.fpri.org/article/2017/07/fighting-disinformation-baltic-states/.

Spriņģe, Inga, and Sanita Jemberga. April 6, 2017. "Sputnik's Unknown Brother." *Re:Baltica*. https://en.rebaltica.lv/2017/04/sputniks-unknown-brother/.

Swedish Ministry of Defense. 2015. "Sweden's Defence Policy: 2016 to 2020." https://www.government.se/globalassets/government/dokument/forsvarsdepartementet/sweden_defence_policy_2016_to_2020.

The European Centre of Excellence for Countering Hybrid Threats. "What Is Hybrid CoE?" Accessed March 20, 2019. https://www.hybridcoe.fi/what-is-hybridcoe/.

Tucker, Joshua A., Andrew Guess, Pablo Barbera, Cristian Vaccari, and Alexandria Siegel. March 2018. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature." *Hewlett Foundation*.

Warwick, Alice, and Rebecca Lewis. 2017. "Media Manipulation and Disinformation Online." *Data & Society Research Institute*.