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

The EU's Common Foreign Security Policy: The Case on Russia's Spread of Disinformation and Election Fraud

Mary Paige Van Kuiken

Abstract

Within the past ten years, Russian election interference has escalated, affecting multiple countries across Europe as well as in the United States. The European Union's (EU) Common Foreign Security Policy (CFSP) was created with the intention to promote international peace and security, however in its current state it cannot address the spread of disinformation that is taking place today. Particularly in Eastern Europe, the amount of interference from Russian media that is taking place is a threat to security, both on a national and EU level. In this paper, we seek to determine to what extent Russian disinformation and election interference has affected European security, and to a larger extent, the world. To do this, we examine cases from Eastern, Central, and Western Europe. Based on the study of trends in disinformation campaigns promoted by Russia, the paper provides an analysis of the CFSP and its shortcomings, particularly regarding the increase of disinformation on a global level.

Written for Topics in Foreign Policy and Internal Security (Prof. Aderito Vicente)
Presented at the JMU – MWP 13th Graduate Symposium,
7 April 2020

Introduction

Within the past ten years, election interference has escalated, affecting many countries across Europe and in the United States (U.S.). This shows that although it has been recurring across different democratic elections globally, the exact definition is still unclear. The 2016 U.S. elections served as a benchmark case in recognizing modern election interference; specifically, the use of social media to influence voters and spread false information. In recent years, there have been multiple instances of interference in the other smaller scale, national European elections. (Gilles 2019) An important question in this case study is why is the Russian government interfering in European elections? How will this interference benefit Russia's agenda and to what extent has this impacted the security of Europe, and to a larger extent, the world?

The newest focus of Russian efforts to interfere in elections appears to be on the Balkans and West European elections, but hybrid activities in the Western and Central Europe, Ukraine, and other countries globally also persist. The European Union itself has also been the subject of a disinformation campaign from the Kremlin, acting to discredit the democratic validity of the institution. The Russian government values cyber activity as a key role in how the government and military operates. They have established troll farms across Russia that exist purely to spread disinformation across different social media platforms. These troll farms have immense amounts of funding from the Russian military; they are constantly putting out new false information intended to disrupt democratic elections across Europe and the world. Within the evolution of cyber activity, the Russian approach to the relationship between information warfare and a traditional state of war is interesting because of the relationship between peace and military action. According to an analysis conducted in 2011, the divide between war and peace can be conveniently broken down in cyberspace. This damage, particularly the spread of disinformation through different media platforms, can be done to an adversary without formally crossing the line between war and peace. (Gilles 2019)

According to the Rand Corporation, Russia spreads propaganda to Russian speakers in the Baltic states, Ukraine, and other nearby states through a variety of means, including traditional and social media. Particularly in Eastern Europe, Russia has used this outreach to inspire dissent against neighboring governments, the North Atlantic Treaty Organization

(NATO) and the European Union (EU). These information operations, which bring back the Soviet-era "active measures," appear to be an increasing priority within the Kremlin, as it spent over $1.1 billion on media disinformation campaigns and troll farms in 2014, increasing its spending on foreign-focused media in 2015. The Kremlin's social media campaigns intertwined with its information operations that involve traditional media, because of traditional news stories being crafted and disseminated online. (Todd C. Helmus, Bodine-Baron and Radin 2018)

The hybrid war tactics that Russia uses today, however, are not closely related to those used during the Cold War. Even if Russia had similar information operations previously than they have access to today, the tactics have evolved dramatically. The volume and ambition of Russian information campaigns today are assisted by the existence of the internet, news sites, and social media, which didn't exist twenty years ago. Using cyber operations is also fairly new. Russia's evolved use of cyber and information technology to gather and use information to influence who they wish is astounding. Because Russia and the world are much more closely interlinked than they were during the Cold War in terms of partnerships and treaties, and the internet, it is faster and easier for Russia to penetrate Western societies. (Gilles 2019)

Europe has found that it is difficult to prevent interference and foreign meddling operations, as there is a functional grey zone where these operations take place. This makes it more difficult to attribute responsibility to one specific government agency. For example, Russia's military intelligence agency is responsible for the gathering of information and digital spying, however other criminal groups and hacking collectives are responsible for the development and deploying of the malware that is used in election hacking. The relation between these groups is difficult to distinguish, making it difficult to know who specifically is carrying out these attacks. This is done intentionally, ensuring that Russia cannot be pinpointed for their interference. Russia's social media disinformation campaign is formidable. Before the Italian election in March 2018, evidence shows that bots were responsible for 15 percent of Twitter activity promoting far-right and populist candidates. The goal of these bots is to create a trend that becomes a headline, influencing more and more people to believe in a cause or a candidate. (Chertoff and Rasmussen 2019)

This paper seeks to understand to what extent Russia has influenced Europe's elections through disinformation campaigns, and what their goal is in doing so. How does this impact

European security, and what can Europe do to defend themselves against these interference campaigns?

Methodology

This paper analyzes the competence of Europe's Common Foreign Security policy and how it may hinder future defense policies of the European Union, particularly regarding the growing need to address Russia's increased disinformation efforts in Europe. This paper uses intra-case analysis to review different cases of disinformation and election interference within the European Union. Using both primary sources and peer-reviewed secondary sources, it has been possible to grasp the range of Russian interference in the Balkan states and Western Europe. When comparing Eastern Europe to Central and Western Europe, Russia used regional and cultural differences to their benefit, pitting these differences against each other, creating divisions. What these countries had in common, however, was an overarching theme of anti-EU and anti-NATO sentiment. Although through slightly different techniques, Russia uses the same rhetoric and techniques in the Eastern Bloc as it does in Western states, with the same aim of creating a polarized and weakened Europe.

Literature Review

This paper will now turn to existing literature regarding the European Union's Common Foreign Security Policy and Russia's spread of disinformation and explain how my research will fit into existing literature. As stated at the beginning of the paper, election interference and disinformation has increased over the years, calling into question the functionality of the CFSP.

The European Union (EU) has become more involved in finding methods to combat the destabilization challenges in cyber activity, such as disinformation and cyberattacks. The EU's response to these hybrid threats can be analyzed by two different policy instruments. The first one, according to Giumelli, Cusumano, and Besana, is that the EU has responded by using its soft power. Soft power involves the ability to influence governments or states without the use or threat of force. This use of soft power has been increasingly adopted by the EU since 2015 in response to misinformation campaigns. The second type is a more traditional, "hard action" that involves the implementation of sanctions and other restrictive measures. Strategic

communication and sanctions are important aspects of countering hybrid threats imposed by Russian media. Policy instruments, such as sanctions and other strict restrictive measures, require especially close cooperation among military and civilian actors. The authors state that strategic communications and sanctions are the most necessary parts of the EU's responses to these emerging hybrid threats and the importance of a common, comprehensive approach to countering them. (Francesco Giumelli 2017)

According to research conducted by Margaret Taylor, European democracies have faced foreign interference in their elections for years, and the primary threat has always been Russia. In the early 2000s, when President Vladimir Putin merged his power in Russia and became the president, he turned his attention to focus on the former states of the Soviet Union and the former Communist countries of Central and Eastern Europe. He intended to pull those countries away from Western-style democracy and encourage them to return to Russia's powerful sphere of influence. He began his campaign of anti-Western democracy here, in an attempt to pull these Balkan states back into the sphere of Russia. After many of these countries joined the European Union and solidified their standing as democratic nations, President Putin shifted his focus towards weakening NATO and the EU. He began disinformation campaigns intended to discredit politicians and democratic institutions, such as free and fair elections and independent media. (Taylor 2019)

In 2019, President Putin made his opinions on Western-style democracy very clear, stating that "The liberal idea" or the dominant western ideology since the end of World War II which includes things like multiculturalism, the rule of law, and respect for human rights—has "become obsolete" and "outlived its purpose." Putin intends to weaken democracy across Europe, and the world, by installing similarly thinking political allies in the highest ranks of government across Europe. By supporting far-right and nationalist parties and leaders, he has the power to influence European democracy and further his goal of establishing Russia as a global power. (Taylor 2019)

The impact of Russia's disinformation operations globally is difficult to measure. Russia's information campaigns appear both modern and sophisticated; pushing boundaries of the digital age, and reminiscent of the old school active measures used in the Soviet era. Social media is the most prominent use of spreading disinformation. In 2017, Russia had exploited Facebook as part of its information campaign for the 2016 United States (US) election.

Through the Internet Research Agency, Russia created multiple Facebook pages that were created with the intention to exploit and expand certain social divisions within the United States that included racial tensions, religion, political affiliation, and class. (Todd C. Helmus, 2018) These pages used Facebook's advertising algorithms to target the ads to specific regions and groups that were viewed as most vulnerable to the intended message. Russia created a "Blacktivist" page, an extreme version of the Black Lives Matter movement that intended to divide the already vulnerable democratic party. Posts on this page incited violence and encouraged voters to resort to whatever means necessary to defend themselves against the "corrupt criminal justice system." Another example is the page "Being Patriotic," which intended to rally Americans against refugee populations seeking asylum in the United States. It also posted attempts to dupe audiences into believing that federal employees were seizing land from private property owners. These posts intended to create a divide between citizens not only among each other, but also between them and their government, inciting anger at how they were supposedly being treated. (Taylor 2019)

EU Action and Europe's CFSP

In May 2019, ahead of the EU's elections, Europe was doing everything in its power to prevent the spread of disinformation over the internet and stop election hacking from taking place. Security experts claimed that there had been attempted interference in months before the election. There has been a sudden rise in Russian state-sponsored hacking against European governments in the past months. The rise of nationalist and populist groups across Europe, particularly the Eastern Bloc, has increased the potential for Russia's disinformation efforts through social media outlets. The European Union does not have its own intelligence service and instead relies on the national government to provide information. It is important to note that the hackers in the Russian government work mostly as an intelligence agency for Russia, so they are gathering geopolitical data and sharing information with the Kremlin. (Foy, Murgia and Peel 2019)

These actions, and the implications that came with Russia's interference, forced the European Union to reevaluate its common foreign and security policies. The European Union established the Common Foreign Security Policy (CFSP) to preserve peace, strengthen security,

promote international cooperation and development. It was also intended to merge democracy, and the rule of law, respect for human rights and fundamental freedoms into the CFSP, promoting western ideals on a global level. (European Parliament 2018) The Common Foreign Security Policy was originally established in the Amsterdam Treaty as a Europe wide alternative to NATO. Two separate pillars created for justice and home affairs policies and the Common Foreign and Security Policy rarely generate true legislation. Decision-making within both of these policies is intergovernmental and unanimity is required to pass votes for almost everything. (European Parliament 2018)

This treaty became re-worked into the Lisbon Treaty of 2007, the most recent treaty outlining the fundamental workings of the EU. According to the Treaty provisions, creation of a European External Action Service (EEAS) is the first step before they can enforce a real foreign policy and establish a High Representative. The High Representative regularly consults Parliament on the principal aspects and the choices of the CFSP to inform Parliament on the evolution of policies. This means that the Parliament's opinions and thoughts are an important factor in this decision making. Parliament holds bi-annual debates on the CFSP and CSDP based on annual progress reports. Questions and recommendations are then posed to the Council or the High Representative. (Troszcynska-VanGenderen 2016)

The problem with the CFSP, however, is that the EU, instead of attempting to improve relations with its external suppliers through transparency, left it to the member states to act accordingly. The European Union has made many attempts to reform the existing voting procedures, which could facilitate a more common and civil agreement, however member states have been reluctant to give up this feature, claiming it is their national and sovereign right. (Foy, Murgia and Peel 2019) The Treaty of Lisbon kept the use of Quality Majority Voting (QMV), or majority by two-thirds, in some circumstances. Primarily, when the European Council has reached a unanimous decision relating to the EU's "strategic interests and objectives," the Council can use QMV to make decisions based on a unanimous decision made on the first round of decisions. (Foy, Murgia and Peel 2019) There is a safety measure that has been built into Article 31(2) Treaty on the European Union (TEU), allowing a Member State to call up national policy, a decision by unanimous vote by the European Council. (Wagnsson and Hellman 2018)

Because the CFSP is intergovernmental, the regular jurisdiction of the European Court does not apply. However, even without any legal obligation to act under the treaty, the political

obligation still stands. The difficulty of upholding the treaty is that the larger Member States do not have much to fear from political sanctions. The Commission and European Parliament have very limited roles in CFSP. The European Parliament has a right to consult on the main aspects and basic choices of CFSP, but the Council is not typically obliged to consider its views. (Archick 2018)

The CFSP in its current state is not strong enough to combat the election fraud and spread of disinformation that has taken place globally. In countries such as France and the United Kingdom (UK), the rise of populist far-right parties can, and has, created many difficult situations for the European Union. In the 2016 "Brexit" referendum, Russian bots and Twitter accounts played a large role in the decision making of the citizens of the UK. Russia's goal of a de-unified Europe with leaders that will allow Putin to have a global influence is becoming more of a possibility. (politics.co.uk 2018)

In its current state, the CFSP has established five goals of the EEAS: first; the EU intends to fully implement the Minsk agreement, as this is a key element of any substantial change possible among the EU and Russia. The second goal is to strengthen relations with the EU's Eastern partners, particularly Central Asia. Third, the European Union must strengthen its internal EU resilience, especially regarding hybrid threats and strategic communication. The fourth principle is the need for engagement with Russia, both on foreign policy issues, especially Iran, Syria, or the Middle East Peace Process, but also migration, counter-terrorism, and climate change. (Euractiv 2012) It is also very important to focus on other areas where there is an identifiable EU interest. This relates to the fifth principle, which elaborates on the necessity of willingness of member states to support the Russian civil society while engaging and investing in contracts and exchanges. (Euractiv 2012)

Three of the EU's regimes of restrictive measures, including travel bans, asset freezes on individuals and entities, and economic measures, will be subject to review in the coming year. The EU has also emphasized the need to challenge Russia's ongoing disinformation campaigns. The current CFSP is not strong enough in its capabilities, especially because of the unanimity clause that prevents important policies from being enacted. (Council of the European Union 2017)

The European External Action Service (EEAS), which carries out the EU's CFSP, has established an action plan of disinformation and focuses on how to deal with disinformation both within the EU and in its neighborhood. Established in 2015, the task force promotes an improved EU capacity to predict, address, and respond to disinformation from Russia. Efforts to strengthen the Strategic Communication Task Force of the EEAS are important players in this plan. Other actions focus on strengthening coordinated and combined responses to disinformation, mobilizing the private sector to ensure it delivers on its obligations in this field, improving the resilience of society in response to challenges that disinformation creates. (Europa 2018)

While the EEAS has combated the spread of disinformation in Europe, there is not enough action being taken. This task force focuses on promoting European values, particularly in the Eastern Neighborhood, while also identifying and exposing disinformation. Countries such as Germany and France have established national laws and strategies to reduce the amount of disinformation that spreads, but the EU needs a common policy that covers all twenty-seven member states, so they are all equally protected. (Europa 2018)

The CFSP's weakness is primarily the member states, who are not a collective union, but rather 27 individual countries. The reason for this is that the national interests of each country transcend the collective vision for the EU. These member states have different perspectives of world issues, and their national interests impede their collective approach in international affairs. This is because while they share common goals being a union, they have their own national interests which diversified in nature due to the expansive geographical and cultural identities of Europe. Often when dealing with policy matters and countries with varying interests, member states do not show their inclination to accept the responsibility, therefore leaving other member states to bear the burden. (Council of the European Union 2017)

Left in its current state, the CFSP will leave Europe divided, unable to create any foreign policy due to disagreements and third country loyalty. It will not be possible to pass a strong policy against Russia with Cyprus, Greece, and Hungary's current relationship with the EU, and their voting power in the CFSP. This could have drastic consequences for Europe, which is facing changing hybrid warfare from Russia almost daily, with challenges such as social media, news sources, and election fraud that has already happened in elections across Europe. (Hellquist 2016) The EU Member States must either respond to the fundamental challenges that have been seen above together, or they must shape their futures and policies individually. There is a large

gap between rhetoric and action that the EU must address before the CFSP can take any strong actions. (Euractiv 2012)

Case Study

The governments and citizens of Estonia, Latvia, and Lithuania, often referred to as the Baltic states, see daily Russian strategic information operations and propaganda through news media and social networks. These are part of campaigns created to undermine trust in the democratic institutions of the West, while generating social tensions. The final goal is to destroy confidence in the North Atlantic Treaty Organization (NATO). There are many Russian speakers within the Baltic states, due to their history and proximity to Russia. Thirty-five percent of Latvians speak Russian as their primary language, while almost thirty percent of Estonians speak the language. Russia aims to pit the Russian-speaking populations in the Baltic region and Ukraine against their neighbors to divide and ultimately conquer. (Foster 2019)

These countries are vulnerable because of their proximity to Russia, and can see variations of hybrid, and full-scale hackings and disinformation attacks by Russian operatives. (Flanagan, et al. 2019) Social media appears to have become Russia's weapon of choice. The efforts that support the goals and objectives of the myriad of actors fighting in the large number of social networks can inform decision making of relevant actors. It is also easily available and accessible. The act of creating fake accounts to show or implicate support for a figure or idea is most often used by Russia. This "warfare" is continuously ongoing and is almost impossible to detect with the current technology that is employed. It is also very difficult to identify the source, as often this hybrid warfare is occurring from several sources simultaneously. (NATO 2019)

Russia's intention has three goals with its disinformation propaganda that it shares to the Baltic States. They begin by describing these states as fascists, who are violent human rights offenders. They even generate fascist demonstrations, sending in agitators from Russia. They also portray a nostalgic image of the former Soviet times, arguing that the Baltic government has been unable to manage their economy or their citizens since becoming independent and

joining the EU. Lastly, they describe the West and NATO negatively, creating stories of NATO attacking innocent civilians and arguing that Baltic independence was purely the result of Western scheming against Russia. (Caryl 2017)

Russia's news sources, such as Sputnik and RT, are available in these states and play sponsored information in Russian on a loop. The media sources are primarily aimed at older generations, who identify more as Russian and may be moved by Russia's propaganda, reminding them of the Soviet Era. Russia's primary goal is to polarize the population. Along with polarization comes weaker elected officials and instability. (Foster 2019)

After Russia's illegal annexation of Crimea in 2014, the EU has had concerns that the Baltic states might become vulnerable to similar hybrid warfare campaigns. These states have been fighting Russia's information warfare for over twenty-five years however and know how to combat these issues. Many experts from the Baltic region have stated that attempting to disprove everything that has been posted online is not the right thing to do. According to the head of the Estonian foreign intelligence service, "Russia has been active. The West has been reactive." (Caryl 2017) Instead, countries like Estonia and Latvia are strengthening their cyber defenses.

The number of EU citizens who follow news on social media grows year by year, by an average of 46 percent in 2016. Russia diligently continues with its hybrid war against the EU and Central and Western Europe as this number rises. The migration crisis of 2015 served as a large weapon for Russia's disinformation and interference campaign. Both the magnitude and the effects of the campaign on Europe's societies has been unprecedented, reaching the level of mass-hysteria. This crisis influenced the public's perception of threat and danger, decreased support for the EU and the mainstream political parties and politicians, while increasing support for extreme-right groups and national solutions rather than common European ones. (Nič 2018)

In the 2019 European Union elections, Russian groups used disinformation campaigns that reduced the voter turnout to change the public opinion. The European Commission and the bloc's foreign policy and security team discovered that Russian-linked groups and other non-state actors had worked hard to discredit the European Union through Facebook, Twitter, YouTube, and other social networking sites. These media sites claimed to shut down thousands of bot accounts that were touting anti-EU and NATO rhetoric. (Apuzzo and Satariano 2019)

Social media campaigns like these are common during election seasons. They question the EU's democratic legitimacy while increasing the attention of sensitive topics in public debate.

such as migration, national sovereignty, and values. The channels and disinformation strategies that Russia uses depend largely on the country that they are impacting and the target group of their message. These messages tend to center upon polarizing the community. This attack was intended to undermine the EU's legitimacy as a supranational institution, and as a democratic body. (Chertoff and Rasmussen 2019)

Russia has been known to impact votes in Europe before. In 2016, the "Brexit" referendum saw high levels of Russian disinformation and interference. The outcome of the vote was close, with 52 percent of voters in favor of leaving the EU and 48 percent opposed to it. It was later established, however, that an army of Russian trolls sent thousands of messages and posts with the hashtag #ReasonsToLeaveEU on the day of Britain's referendum on membership of the European Union. While many parts of the Brexit referendum are still being investigated, Russia manipulated social media trends to help influence the growing divide between Britain and the EU. It is unclear to what extent Russia interfered in the election, but Russia is intent on creating a divided Europe that has no need for common defense policies. (Kraemer 2020)

In 2017, France's President Emmanuel Macron was the target of Russian hacking prior to the election. A week before the final election was to take place, Macron's campaign announced it that someone had hacked thousands of emails and private communications., leaking them to the public. Macron was an independent centrist who was campaigning against the far-right populist and National Front leader Marine Le Pen. La Pen has enjoyed considerable Russian financial support and from favorable coverage in state-run Russian media for years. (McAuley 2017) While Macron won the election, his vows for European unity and collaboration within the EU were not what Russia wanted to hear, and Le Pen's divisive racism and xenophobia aligned with Russia's goals of dividing Europe. (Wagnsson and Hellman 2018)

Particularly in Eastern Europe, in the Czech Republic and Slovakia, the rise of far-right and nationalist parties has been in part because of social media campaigns and widespread racism and xenophobia. In the Czech Republic, a quarter a Czechs trust pro-Kremlin media sources more than they trust traditional news and media. About forty-eight websites that spread Russian disinformation are visited over five thousand times a month. (Helmus et al., 2018)

Milos Zeman, the president of the Czech Republic, has spoken out in favor of Russia. He often compliments President Putin, claiming that the Western states in the EU are looking to blame Russia with no cause. As the only one of many senior Western politicians, he

defends the seizure and annexation of Crimea by the regime of Vladimir Putin, and denies Russian forces in eastern Ukraine, calling for all sanctions to be lifted. (Gilles 2019) Mr. Zeman was only narrowly reelected in 2018, with his opponent's campaign promise of "reaffirming ties to the west" was subject to many interference and disinformation campaigns. Mr. Zeman also received large amounts of money during his campaign from an undisclosed source, which Zeman himself claimed could "quite possible be Russia." (Editorial Board 2018)

Russia sees Slovakia as the only Visegrad country that could conceivably leave NATO, so they are focusing their attention there. In Central and Eastern Slovakia, support for NATO is only at 50%. Slovakia proved to be the most pro-Russian, followed by Hungary and the Czech Republic. In Slovakia, 28% of the population had positive sentiments towards Russia, directly correlated to the Russia-related news that is disproportionally covered by pro-Russian disinformation sites. This number is also because of the far-right and paramilitary groups that reminisce on the historic ties between the two countries and want to see these ties restored. Russia uses nostalgia of the Communist Soviet past to promote their own narratives, through their own news sources and social media. (Caryl 2017)

The main purpose of Russia's disinformation campaigns and hybrid warfare across Europe is to undermine its opponents, in this case the EU. Rather than promoting Russia and Russian ideals, the Kremlin seeks to gradually decompose the institutional framework and democratic integrity of Europe. In both Central and eastern Europe, the target of these attacks has been NATO and the EU, and Russia often depicts itself as the only rational actor. They portray themselves as being the unrecognized or misunderstood peacemaker, and often the necessary savior that is desperately needed in global politics today. (Chivvis 2017)

Russia uses social media networks to their benefit, as they can bypass the traditional media sources and have a direct influence on public opinion. They can promote fake, radical news stories that support their position of being the strongest and only rational actor in the global political arena. By polarizing the EU, Russia has a stronger chance of implementing its influence into these communities. Eventually, the goal is to have global influence over a de-united Europe and become the acting hegemon. (Gilles 2019)

Conclusion

Europe's Common Foreign Security Policy was created intending to combat threats to Europe's peace and democracy. When the EU needs it most, however, it is not useful, and can barely be implemented. The Common Foreign Security Policy must change to address the changing hybrid threats that the EU sees today. As Russia adapts to changing technology and online platforms, using social media networks to question the EU's democratic legitimacy, the EU must also adapt, or it will leave Europe divided, with no security policy to protect it.

The EEAs task force focuses on countering disinformation, but it does not expand further to take direct action against Russia or get ahead of the problem. Many Eastern European countries, like Estonia, have been so successful in warding off Russia's relentless hacking because they are one step ahead. The European External Action Service's action plan to combat disinformation is a step in the right direction, but there must be more action taken to face the inevitable interference that will happen.

Russia's disinformation and interference campaigns have one aim- to polarize the communities in which they target. By constantly being behind and attempting to disprove post after post, there is no hope in combatting Russia's massive disinformation platform. In Eastern Europe, the goal is to cause divisiveness between native Russian speakers and those who aren't, while constantly inundating the citizens with anti- NATO and European Union propaganda. The only way to truly combat this is to get ahead and know how to block the bots and channels of disinformation strategies. In Central and Western Europe, Russia aims to polarize by supporting far right and nationalist parties that challenge the EU's democratic values. (Chivvis 2017)

While they vary in extent and value, Russia's disinformation campaigns over the past ten years have grown exponentially, adapting to rapidly changing technology. This demonstrates Russia's intent to create a Europe that is so divided that a common security policy will not be necessary, as there will not be a common Europe in which to create policy around. Europe's security has already been impacted through the recent elections at the EU level, and the referendum held in the UK.

Having seen a rise in nationalist and far right parties across the European Union, disinformation campaigns work, regardless if they are true. This seems to be Russia's goal—to create a polarized Europe that has no means of protecting itself, thus allowing Russia to increase its influence and power. If the EU does not have an active and hybrid Common Foreign Security

Policy, this may become a reality—without the European Union adapting to the technological changes happening around it, there will be consequences.

References

Alina Polyakova, Spencer P. Boyer. 2018. "The future of political warfare: Russia, the West, and the coming age of global digital competition." *Brookings Institute.* https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2018-07/Political%20Warfare.pdf.

Apuzzo, Matt, and Adam Satariano. 2019. *Russia is targeting Europe's elections. So are far-right copycats.*https://www.nytimes.com/2019/05/12/world/europe/russian-propaganda-influence-campaign-european-elections-far-right.html.

Archick, Kristin. 2018. "European Union: Current challenges and future prospects." *HeinOnline*. https://heinonline.org/HOL/Page?collection=congrec&handle=hein.crs/crsmthzzbzv0001&id=3&men_tab=srchresults.

Carroll, Oliver. 2020. "EU accuses Russia of disinformation campaign." *Independent* . Archive of European Integration.

Caryl, Christian. 2017. *If you want to see Russian information warfare at its worst, visit these countries.* https://www.washingtonpost.com/news/democracy-post/wp/2017/04/05/if-you-want-to-see-russian-information-warfare-at-its-worst-visit-these-countries/.

Chertoff, Michael, and Anders Rasmussen. 2019. "The unhackable election: What it takes to defend democracy." https://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=6&sid=4b0b02b0-c7e3-4441-b347-e43bc584d238%40sessionmgr4008.

Chivvis, Christopher. 2017. " Understanding Russian “Hybrid Warfare” And what can be done about it." *Rand Corporation.* https://pdfs.semanticscholar.org/d72f/627dfacb42ce811b203f04431b172b029b66.pdf.

Council of the European Union. 2017. *CFSP Report – Our Priorities* . https://eeas.europa.eu/sites/eeas/files/st10650_en-cfsp_report_2017.pdf.

Daniels, Laura. 2017. *How Russia hacked the French election*. https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.

Dempsey, Judy. 2018. *Does Europe have a Russia policy?* https://carnegieeurope.eu/strategiceurope/75924.

Editorial Board. 2018. *From the Czech Republic, a warning for our midterms: The Russians are still meddling.* https://www.washingtonpost.com/opinions/global-opinions/from-the-czech-republic-a-warning-for-our-midterms-the-russians-are-still-meddling/2018/01/29/4498a748-0517-11e8-b48c-b07fea957bd5_story.html.

Euractiv. 2012. *No common, no security, no policy and all foreign.* https://www.euractiv.com/section/science-policymaking/opinion/no-common-no-security-no-policy-and-all-foreign/.

Europa. 2018. *Action Plan on disinformation: Commission contribution to the European Council* . https://ec.europa.eu/commission/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en.

European Parliament. 2018. "Foreign policy: aims, instruments and achievements." *EuroParl.* https://www.europarl.europa.eu/factsheets/en/sheet/158/foreign-policy-aims-instruments-and-achievements.

Flanagan, Stephen, Jan Osburg, Anika Binnendijk, Marta Kepe, and Andrew Radin. 2019. *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance.* https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2779/RAND_RR2779.pdf.

Foster, Kendric. 2019. *A Walk Down Baltic Avenue.* http://harvardpolitics.com/world/a-walk-down-baltic-avenue/.

Foy, Henry, Madhumita Murgia, and Michael Peel. 2019. "EU Scrambles to stop Russian interference ahed of May elections." *Financial Times.* https://www.ft.com/content/d8205ea0-3a6a-11e9-b72b-2c7f526ca5d0.

Francesco Giumelli, Eugenio Cusumano , Matteo Besana. 2017. "From strategic communication to sanctions: The European Union’s approach to hybrid threats." *SpringerLink.*https://link.springer.com/chapter/10.1007/978-3-319-60798-6_8.

Gilles, Kier. 2019. "The next phase of Russian information warfare." *NATO Strategic Communications Centre of Excellence.* https://s3.amazonaws.com/academia.edu.documents/51448772/keir_giles_public_20.05.2016.pdf?response-content-

disposition=inline%3B%20filename%3DThe_Next_Phase_of_Russian_Information_Wa.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL.

Haukkala, Hiski. 2019. "What went right with the EU's Common Strategy." *Rethinking the Respective Strategies of Russia and the European Union.* https://www.files.ethz.ch/isn/10733/doc_10764_290_en.pdf#page=63.

Hellquist, Elin. 2016. "Either with us or against us? Third-country alignment with EU sanctions against Russia/Ukraine." *Cambridge Review of International Affairs* 997-1121.

Kraemer, Daniel. 2020. "BBCNews." *Russia report: when can weexpect it to be published.* February. https://www.bbc.com/news/uk-politics-51417880 .

McAuley, James. 2017. *France starts probing 'massive' hack of emails and documents reported by Macron campaign.* https://www.washingtonpost.com/world/macrons-campaign-says-it-has-been-hit-by-massive-hack-of-emails-and-documents/2017/05/05/fc638f18-3020-11e7-a335-fa0ae1940305_story.html.

NATO. 2019. *Internet trolling as a hybrid warfare tool: the case of Latvia.* https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0.

Nič, Milan Šuplata and Milan. 2018. *Russia's Information War in Central Europe: ew Trends and Counter Measures.* https://www.europeanvalues.net/wp-content/uploads/2016/09/russias_information_war_in_central_europe.pdf.

politics.co.uk. 2018. *Common Foreign and Security Policy.* https://www.politics.co.uk/reference/common-foreign-and-security-policy.

Scheidt, Melanie. 2019. "The European Union versus Extenal disinformation campaigns in the Midst of Information Warfare: Ready for the Battle?" *Archive of European Integration* 2-33.

Schuette, Leonard. 2019. *Should the EU make foreign policy decisions by majority voting?* https://www.cer.eu/publications/archive/policy-brief/2019/should-eu-make-foreign-policy-decisions-majority-voting#section-10.

Taylor, Margaret. 2019. *Combatting disinformation foreign interference in democracies: Lessons from Europe.* July. https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/.

Todd C. Helmus, T, Elizabeth Bodine-Baron, and Andrew Radin. 2018. "Russian social media influence: Understanding Russian propoganda in Eastern Europe." *Rand Corporation.* https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf.

Troszcynska-VanGenderen. 2016. *The Lisbon Treaty's provisions on CFSP/CSDP State of implementation.* https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/570446/EXPO_IDA(2015)570446_EN.pdf.

Wagnsson, Charlotte, and Maria Hellman. 2018. "Normative Power Europe Caving In? EU under Pressure of Russian Information Warfare." *Journal of Common Market Studies* 1161-1177.