Policy Paper

Securing Democracy: Addressing the Threat of Russian Disinformation Campaigns in Liberal Democracies in the EU

By Leon Wiskie

February 2024

THE GLOBAL POLICY HORIZONS LAB

Empowering Evidence-Based Solutions

For a Better World

Webster University
470 E Lockwood Ave, St. Louis, MO 63119, USA

Introduction

The end of the Cold War in 1991 provided an opportunity for Russia and the European Union (EU) to reorganize their bilateral relationship. They nurtured close ties for over a decade, but the Russian-EU relationship has deteriorated recently. Disagreements have arisen over issues such as NATO expansion, EU enlargement, the 2006 Russia-Ukraine gas disputes, the Russia-Georgia conflict in 2008, cyber-attacks, and 'color revolutions' (Kapoor, 2021).

The annexation of Crimea in 2014 marked a significant turning point in the relationship. The EU and Russia have opposing interpretations of the crisis, extending beyond Ukraine, and reflected in their policy announcements in 2016 (Kapoor, 2021). Moscow shifted its focus to China and Asia due to the EU's disregard for Russian interests, making the EU a strategic challenge for Russia. And the EU isolated Russia.

The invasion of Ukraine by Russia in 2022 resulted in sanctions that even further isolated Russia from the EU. The EU increased economic sanctions and supports Ukraine's defense. This further strained EU-Russia relations, resulting in an extended low-intensity conflict; a conflict between the NATO and Russia below the threshold of war. As the NATO article 5 clause remains, the EU's main deterrence against Russia military aggression. However, a military confrontation between NATO and Russia on the European continent remains, for now, less likely. Russia is resorting to other means to weaken military support to Ukraine and implementing tactics to nullify the effects of foreign policies against its interests. These tactics are known as gray zone tactics. The effects of these tactics have destabilizing consequences for liberal democracies.

I argue by prioritizing the enhancement of societal resilience, rather than relying on strategies like content censorship and restrictions on (social) media platforms, we can effectively address the challenges faced by our society.

Many believe that strong liberal democracies in the western EU are impervious to gray zone tactics, such as foreign influence in democratic processes using disinformation campaigns and the spread of propaganda. However, I believe these tactics are effective, although the effects of these tactics are less visible to EU policymakers. In this article, I will focus on several examples of the use of these tactics against Eastern European countries like Poland and Hungary and western EU states like the Netherlands, France, and Germany. The Baltic States share a border with Russia and have strong historical and cultural connections. However, in this article, I will not focus on the Baltics states because of these specific dynamics between Russia and the Baltics. In this regard, they differ strongly from other EU states.

I argue that disinformation campaigns are as destructive in strong states in the west of Europe as in weaker states in the Southeast of Europe and at the EU-Russian border. Current research shows Russia's main tactic is the manipulation of other states' digital information space (Morris et al., 2019). The RAND Corporation notes that Russian gray zone tactics are aimed at political institutions in the EU (Morris et al., 2019). I believe this article is relevant because these tactics have destabilizing effects on the political cohesion of the EU and its member states.

Furthermore, I argue that there are flaws in the current strategy of the EU to limit the effects of disinformation campaigns launched by Russia. This can be observed by researching the causes of societal friction that can be a result of foreign influencing public opinion with malign intend.

This article is aimed at EU states and EU parliament members. These are the policymakers responsible for developing strategies countering disinformation campaigns, specifically focusing on the current conflict between Russia and the EU. The article is structured into four sections: an explanation of concepts such as the gray zone and Russia's modus operandi, an overview of current strategies countering Russian disinformation in the EU, and an analysis of the current shortcomings in these strategies. Lastly, a proposal for a strategy based on societal resilience for liberal democratic nations is presented, along with recommendations for altering strategies in the EU and liberal western democracies like the Netherlands, France, and Germany.

Gray Zone Tactics

In international relations, states employ diverse forms of power to shape their environment to serve their national interest. They influence their competitor’s policies and views, whether they are in proximity or distant. The main instruments of national power are Diplomacy, Information, Military, and Economic (DIME). These instruments of influence are vital to a state's foreign policy, as they determine how a nation navigates its relationships with other countries and international organizations.

Traditional great power competition between the US and USSR changed after the Cold War. Full-scale military confrontation between nuclear-capable states like Russia, China, and the US is less likely, as new conflicts are less likely to be fought through military means due to the unwillingness of politicians to sacrifice life and infrastructure.

Russia and China, as strategic competitors of the EU, employ unconventional tools and tactics opposed to traditional military power and war. These include propaganda campaigns, economic pressure, and the use of non-state entities as part of their foreign policy. These actions do not exceed the threshold of formalized state-level aggression (Carment and Belo, 2020). Rendering a response to these actions in accordance with Article 51 of the UN Charter, utilizing force as retaliation, is deemed illegitimate or problematic.

As Carl von Clausewitz's dictum is often reduced to "war is a continuation of politics by other means" current states are engaging in political actions that have similar effects to war, without direct or indirect military confrontation between superpowers as seen throughout history and recently during the Cold War in Korea and Vietnam.

The new means of conducting foreign policy, without using hard power, are employed by states that are not formally at war but have strategic competition in a geopolitical context. The goal of this competition is to gain political influence, change the current international order, and gain economic advantage over the others.

In this gray zone, which is the concept used to express a state of international relations between war and peace, antagonists employ all means without direct military force or formal military confrontation. Moreover, in this gray zone, there are no constraints on how actors conduct operations to achieve their objectives, both legally and ethically. These operations rely on ambiguity to avoid confrontations between aggressors and their targets (Belo, 2020).

The tactics used to influence relations between nations and shape the sociopolitical realm of other states aim to create a political environment that aligns with their interests. These new types of conflicts are characterized by low intensity and often occur between politically and economically interdependent parties like the US and Russia, and the EU and Russia (Carment and Belo, 2020). This challenges the conventional belief that strong economic relations lead to peace. This is particularly relevant for the current relationship between Russia and the EU, as they have strong economic interdependencies.

Gray zone tactics are now part of foreign policy and military doctrines of states. Especially, nondemocratic states such as Russia and China are actively involved deploying these tactics against democratic states like the US and EU (Gill et al., 2020). Both Russia and China did extensive research on this topic. Russia’s Gerasimov and China's Unrestricted warfare doctrine, both, are examples of hybrid warfare tactics used in both war and peace, and in the space between, the gray zone.

During the Cold War, the main security service of the USSR, known as the KGB, employed various unconventional soft power tactics such as espionage, sabotage, propaganda, and assassination. For instance, political warfare and disinformation campaigns were used against the US and its allies throughout the Cold War (Gill and Goolsby, 2022).

As in the last decades the world became more globalized — meaning a high degree of state interdependence through trade and technology — political warfare shifted to information warfare. During the Cold War, political warfare focused on the influence gap rather than the missile gap (Jensen, 2017). With advancements in information technology (IT), political warfare transitioned to cyberspace—a global, interconnected digital information space used to reach and influence people worldwide. This shift in geopolitics means that proximity is no longer the main factor influencing another state's policies.

This digital information domain, known as cyberspace, is a strategic battleground for states. Jensen explains that cyber operations covertly influence adversaries through online attacks such as intrusions, logic bombs, and denial of service attacks. Additionally, Jensen highlights how traditional political warfare has shifted to focus on the digital information domain (Jensen, 2017). Following the deterioration of Russia-EU relations, the EU has been particularly targeted by disinformation campaigns.

Disinformation campaigns are targeted, organized information attacks on companies, parties, institutions, or individuals. They involve the deliberate dissemination of a large volume of demonstrably false or misleading information – disinformation—on a large scale to manipulate and influence political and election processes. Well-researched examples include the 2016 US elections and the 2017 French presidential elections, where social media platforms were used by Russia and pro-Russian non-state actors to spread false information through troll factories and sock puppets (Kreps, 2020). A troll farm or troll factory is an institutionalized group that operates on the internet to interfere in political opinions and decision-making. These groups can be government agents (state actors) or individuals that align with the ideologies or objectives of their masters (non-state actors). Next to trolls, sock puppets are false online identities, typically created by a person or group to promote their opinions or views.

To conclude, it is evident that the EU's strategic competitors, namely Russia and China, are employing unconventional methods like gray zone tactics and strategies to exert influence. These include propaganda campaigns, economic coercion, and the utilization of non-state actors. These tactics are deliberately designed to avoid confrontation that would trigger a formalized state-level aggression. The presence of NATO and the EU's mutual defense clauses serves as a protective shield for the EU, dissuading traditional conflicts as they would not align with the interests of these competitors. The mutual defense clause ensures that if any member state of NATO or the EU is attacked, all other states are obligated to help to support using all available means at their disposal.

Russian Gray Zone Tactics

After the decline of EU-Russia relations in the last decade, both parties are now competing for political and economic power in Europe. Russia aims to regain influence over its neighboring former USSR states and the European Union (EU). According to RAND research, Russia's objectives include establishing itself as a great power and reducing the U.S. dominant role in the current global order, which could be achieved through hostile measures in Western and Central Europe (Cohen and Radin, 2019). The EU's involvement in this power competition between Russia and the US is significant as they are the EU's major partner.

To regain influence in the EU and its neighboring regions, Russia employs a wide range of gray zone tactics. Its main objectives are to interfere with states' policies against Russia, disrupt EU and NATO expansion and integration, and reduce the effectiveness of the EU. The use of disinformation, propaganda, and cyber-attacks are the most prominent used tactics by Russia. However, some of these methods, like cyber-attacks, have proven less effective in changing states' stance on EU and NATO expansion in Europe (Cohen and Radin, 2019).

The use of these type of tactics is nothing new. The USSR KGB used disinformation campaigns during the Cold War. A strategy that focuses on altering how a target population thinks and how it acts. By influencing public opinion, the KGB was sowing chaos in societies (Jensen, 2017). The current Russian intelligence services like the GRU and FSB renewed these tactics in a digitized world and deploy them against the US, the EU member states and former USSR states like Ukraine.

Russia's current gray zone tactics target EU political stability, economic growth, and social cohesion. The main medium used to influence these factors is the digital information space and the use of information technology (Morris et al., 2019). Research suggests Russia's main gray zone tactic is information warfare. Using disinformation campaigns and cyberattacks provides ample ambiguity and deniability for Russia and are deemed effective (Gill et al., 2020).

As RAND research shows, Russia employs different methods for various targets. Russia exploits the different vulnerabilities that exist in states. RAND defines weaker states as having less developed democracies, weak institutions, and high corruption compared to stronger democracies (Pettyjohn and Wasser, 2019). For example, weaker European Union states, such as those in the Balkans. Other smaller Central European states are more vulnerable to Russian aggression. These weaker EU states in Southeastern Europe are vulnerable to their lower economic development, weaker democratic systems, and favorable Slavic populations (Cohen and Radin, 2019). Cohen and Radin's study highlights that Russia exploits divisions that exist due to economic difficulties, social discontent, and existing ethnic conflict. Several former Yugoslavian states have joined the EU and NATO, which made them a target.

One tactic used by Russia in its near abroad is the Russian language, shared history and culture. In former USSR states like the Baltics and Ukraine, this primarily involves the spread of pro-Russian propaganda aimed at Russian speakers in these regions (Kuczyńska-Zonik, 2021). These tactics exacerbate tensions and encourage ethnic conflicts. According to Cohen and Radin Russia's compatriot policy and Russian language media penetration in this region, such as Russia Today (RT), can escalate tensions in the Baltic States through disinformation operations (Cohen and Radin, 2019).

Stronger EU states like the Netherlands, France, and Germany have increasingly interfered in democratic and political processes over the last decade (Cohen and Radin, 2019). There are well-researched examples where Russia actively interfered in elections in France and Germany by spreading disinformation about the individual politicians and political parties that were involved in these elections. Furthermore, Russia actively supported right-wing political parties in Italy, the Netherlands, Germany, and France. These political parties actively amplified Russian propaganda and are more aligned with Russia's interests, such as preventing further EU integration and NATO expansion (Wesslau, 2016).

In conclusion, gray zone information operations are a complex phenomenon that involves both non-state actors and state actors. Pro-Russian hackers, media outlets, and Russian security services like the GRU and FSB play a significant role in conducting these operations. Moreover, proxies such as Russia Today (RT) also contribute to the dissemination of gray zone tactics. It is important to note that there exists a noticeable disparity in the approaches employed in former USSR states compared to Western European states like the Netherlands, France, and Germany.

Understanding and addressing these differences are crucial for effectively countering gray zone disinformation campaigns in various geopolitical contexts.

EU Strategy Against Russian Gray Zone Tactics

Political stability in liberal democracies is among others based on the rule of law, trust in institutions, and democratic political processes (Carugati, 2020). Eroding trust in these basic tenets of democratic states can be done by influencing individuals through spreading false information. Lately, Russia has frequently employed this tactic, particularly in cyberspace, to disrupt the effectiveness of its strategic competitors' foreign policies.

The EU Foreign interference and manipulation, including disinformation, have been identified as a rapidly growing political and security challenge for the European Union. But also, to its immediate neighborhood (Western Balkans and Eastern Partnership countries) as well as for global security and stability (Caprile, 2023).

For example, there is strong evidence that Russia interfered during several EU member state parliamentary and presidential elections. Issit defines electoral interference as the intentional disruption or influence of the electoral process of a sovereign nation (Issit, n.d.). In 2017, there were numerous examples of foreign interference in electoral processes in EU states. First, there is evidence of various interference attempts in the German elections of 2017. As Germany is one of the main leaders in European politics, influencing German politics has significant effects on EU foreign policy (Stelzenmüller, 2017). A second example is interference attempts by Russia in the elections in the Netherlands of 2017 as the Dutch intelligence service AIVD reports in its annual report of 2018 (Koninkrijksrelaties, 2018). The AIVD claims Russia tried to spread news items that are not true, or partially true, to influence voters in the 2017 parliamentary elections.

The Netherlands has been a major target of Russian disinformation campaigns. One event triggered a strong Russian response. As a passenger flight, MH17 from Amsterdam to Kuala Lumpur was shot down over Ukraine in 2014, resulting in the deaths of all 298 passengers, including 193 Dutch nationals. The anti-aircraft missile that downed the plane was launched from an area in Ukraine controlled by pro-Russian separatists, who received support from the Russian military. The Netherlands investigated this incident and identified the missile launcher was operated by Russian nationals. As a result, the country became a target of Russian propaganda, cyberattacks, and disinformation campaigns aimed at disrupting and discrediting further investigations and interfering with Dutch state affairs.

In response to several disinformation campaigns, the EU adopted a resolution in 2023. This resolution stipulates the different strategies the EU deploys against interference in democratic processes and addresses the risks of disinformation. The strategy focuses on adherence to international norms and legislation, the role of media, and enhancing media literacy (Texts Adopted, 2023).

International Norms and Legislation

In response, the EU and liberal democratic states generally rely on international norms and legislation to deter Russian interventions. The EU and its member states uphold the non-intervention principle, a fundamental concept in international law that restricts foreign nations from interfering in the internal affairs of sovereign states. However, disinformation campaigns are often covert and carried out using proxies (e.g., non-state actors like criminals and groups of activists), making it difficult to attribute responsibility to a state and pursue legal action according to international laws.

To overcome some of these limitations, the EU regulated its information domain. There are various EU regulations focusing on digital services like social media and digital markets. These regulations give regulators the power to intervene in companies that host digital services like social media platforms, one of the prevalent media used to spread disinformation. However, these regulations are not effective. According to Bayer et al., while the draft regulations for the Digital Services Act (DSA) and Digital Markets Act (DMA) offer a promising regulatory scheme, they fall short in addressing the full range of rules required to effectively combat disinformation (Bayer et al., 2021).

The Role of Media

Liberal democracies like the EU states rely on open, free, and independent media. The reliable flow of information is crucial in maintaining democratic processes like elections. However, disinformation campaigns, authoritarian crackdowns on press freedoms, and the decline in local journalism present critical obstacles to this flow.

Above all, there are concerns regarding the public perception of information disseminated by public and private media outlets in the EU. The advent of citizens journalism and social media changed the role of the press and media in society. According to Bayer et al., the disappearance of hierarchies and entry barriers in the traditional media system characterizes the post-truth era (Bayer et al., 2021). This created a new challenge in maintaining a balance between freedom of expression and countering evidently false information in democracies.

The lack of authority and trust in the media creates vulnerabilities in societies. Russian disinformation strategies are focus on creating fear, uncertainty, and doubt that reach every individual. These tactics entail discrediting liberal political views and polarizing groups in society. Russia uses false narratives and spreads them by several media outlets like Russia Today (RT), Sputnik. Furthermore, social media accounts amplify false stories and information on social media channels reaching almost all individuals due to highly digitalized societies in the EU.

One strategy to counter disinformation in the media is the creation of fact-checking entities and regulating information spread on social media platforms. The regulation was aimed at the ability to ban specific content and limiting the access of state actors and non-state actors to social media platforms. For example, in 2017, France put pressure on Facebook to remove

70,000 fake accounts disseminating false information about the elections. They were able to remove them before the voting process, and so interfered with the entities operating these accounts from reaching their objectives (Vilmer and Conley, 2018).

Furthermore, the France government also reacted by revoking the accreditation of Russian state media like Sputnik and Russia Today (RT) for actively spreading propaganda on TV and social media. However, Vilmer and Conley's argue that the decision made by France has been a source of controversy, reinforcing the Kremlin's narrative and giving Russian President Putin an opportunity to discuss freedom of the press (Vilmer and Conley, 2018).

Other states in the EU were also targeted. NATO research shows the effects of Russian information campaigns using media outlets in the Netherlands. According to Bayer et al. Bellingcat's investigation reveals the close affiliation between Bonanza Media and the Russian military intelligence service GRU (Bayer et al., 2021). According to Bellingcat, the media platform founded by Yana Yerlashova and Max van der Werff aimed to disseminate alternative narratives regarding the MH17 crash (Bellincat, 2020).

Media Literacy and Inoculation

Research shows that the most effective strategy to counter disinformation campaigns is critical media literacy. According to Bayer et al., critical media literacy is identified as the most effective tool for combating the impact of disinformation (Bayer et al., 2021).

One of the key strategies in critical media literacy is inoculation. Inoculation or psychological inoculation is a method to counter the negative effects of disinformation. According to Roozenbeek et al., the use of inoculation videos can effectively enhance psychological resistance against common manipulation techniques encountered in online misinformation, benefiting individuals across different ideological backgrounds and cognitive styles (Roozenbeek et al., 2020). Furthermore, Gill et al. argue that promoting effective online hygiene and information practices, including verifying information with trusted sources, is crucial in fostering greater awareness during critical events such as elections (Gill et al., 2020).

Additionally, the EU has introduced initiatives like "EUvsDisinformation" to protect its society from disinformation. EUvsDisinfo identifies and exposes cases of disinformation originating in pro-Kremlin media, which are spread across the EU and Eastern Partnership countries. It actively informs the public about current disinformation campaigns.

However, detecting and identifying disinformation is challenging, it requires cooperation between EU states and individuals' ability to recognize false information.

Weaknesses in Current EU Strategy

Despite EU efforts to limit disinformation, it still impacts trust in democracy and elections.

Above all, the EU noted there is still an increase of foreign-originated disinformation campaigns (Bayer et al., 2021). Making it even harder to counter this problem.

Although not an EU example, former US President Trump openly questioned the results and the legitimacy of political processes during the 2020 elections. This had a significant effect on liberal democracies in general. The spreading of narratives of unfair elections created distrust in liberal democratic institutions in EU member states, as many EU political leaders mimicked others of Trump's strategies in their campaigns.

Other examples were the case of several EU Political figures openly questioning information regarding the COVID-19 pandemic and treatment campaigns and effectiveness. This intensified political debates in EU member states, which were actively exploited by Russia and China (Gill et al., 2020). According to Gill et al. there are various examples of disinformation campaigns that were directed at social media to intensify this debate.

As Pettyjohn and Wasser note, although Russia's gray zone tactics signify its weakness, the West's stronger political, cultural, and social systems will prevail over them if given the chance (Pettyjohn and Wasser, 2019). So there is hope. However, others suggest that the effects of disinformation campaigns on societies are difficult to notice because of the prolonged and low intensity of these operations. Hence, it is challenging to determine who is winning or losing this battle in the gray zone.

In conclusion, the significance of public understanding, perceptions, and demand for free and independent media must not be understated. The effects of disinformation campaigns emphasize the vulnerabilities that exist in highly digitalized liberal democracies within the European Union. As these countries heavily rely on open, independent media sources for news-gathering, which in turn influences the formation of public opinion about society. This underscores the crucial role that free and independent media play in shaping democratic societies and calls for continued support and protection of these vital institutions.

Pressure on Independent Media

The freedom of expression and free press are important parts of international law and EU statutes. However, there are signs that governments in some states are curtailing open and free media. For example, there are limitations on free and open media in Eastern EU countries like Hungary and Poland.

Since 2010, President Victor Orbán is in power. During his presidency, he significantly changed the Hungarian media landscape. In a statement, the Council of Europe expressed their concerns on current heading of Hungary regarding the combined effects of a politically controlled media regulatory authority and government intervention in the media market have eroded media pluralism and freedom of expression in Hungary (Commissioner for Human Rights, 2021).

Next to Hungary, the government in Poland also reduced freedom of press privileges. In a statement by the EU parliament, the parliament members condemned the continuing deterioration of media freedom and the rule of law in Poland. The EU parliament has expressed its concern over the reshaping of the public broadcaster into a pro-government organization, the 'Lex TVN' bill adopted by the Polish parliament. The EU parliament described this bill as "an attempt to silence critical content and a direct attack on media pluralism" that violates both EU and international law (European Parliament, 2021).

Limiting freedom of the press in these EU members states creates vulnerability that can be exploited because freedom of expression and the media are crucial for independent news-gathering. It is a key criterion for European states joining the EU. Furthermore, limiting reporting and the freedom to critic current political leaders polices in the press creates a dysfunctional liberal democracy and enables societal distrust, which can be exploited through disinformation campaigns.

Fact-Checking & Self-Regulation

Democracies depend on open conversations and the free flow of information. However, there always exists a tension between filtering or censoring false information used by foreign entities, such as Russia. This interference (i.e., filtering and censoring) of the information in the media landscape negatively impacts trust in democracies.

Next to filtering and censoring, the use of fact-checking entities is problematic. This includes both the process of fact-checking and the authority of those who do the fact-checking. In many states, media outlets are increasingly distrusted and so is the role of those who are conducting the process of fact-checking.

According to Bayer et al., the misuse of the label "fact-checking" by disinformation agencies undermines independent and trustworthy news sources by denying facts and accusing them of the very behavior they themselves engage in (Bayer et al., 2021).

In a democracy, free conversation among different opinions is essential, and restricting this conversation is detrimental to democracy. The self-regulation for social media platforms and fact checking are creating risk of censoring media landscape, interfering with democratic processes and freedom of information in the EU. According to Bayer et al., disinformation agencies exploit the label of 'fact-checking' to discredit reliable news sources and manipulate facts for their agenda (Bayer et al., 2021).

In conclusion, Berg and Peterson argue that civilians must perceive state intervention and initiatives as legitimate and actively resist outside interference or threats (Berg and Petterson, 2022). A lack of trust in the legitimacy of state intervention in the information space like appointing fact checking entities and applying regulation is detrimental to democracy and creates even more exploitable vulnerabilities.

EU's Challenging Political Landscape

Another factor that makes current strategies against Russian influence less effective is the rise of right-wing nationalist populist political parties in the EU. These political parties are in general

EU skeptic and the EU has seen changes in political landscape in general. In this way, their political agenda align in some degree with Russian interest regarding the EU. In the last decade, there was the rise of nationalist parties in stronger democracies like Germany, the Netherlands, and France.

There are cases that show how targeted disinformation campaigns can influence people's political preferences. According to Meister, the media storm surrounding a fake story about a Russian-German girl, who had supposedly been raped by Arab migrants, highlighted the German government's awareness of Russian manipulation of public opinion and its connection to Russian politics (Meister, 2016).

Events in the Lisa case were aimed at making far-right political parties more attractive to voters. The German security service BND found evidence that the Lisa case was a clear example of a disinformation campaign to disrupt the German political landscape (Meister, 2016). The public opinion regarding immigrants changed. Because a narrative of immigrants committing horrible crimes in Germany resulted in, more people are willing to vote against immigration and align with a more right-wing political agenda, making them more powerful in local parliaments and government. This creates a more divided political landscape in EU parliaments, which makes it harder to gain consensus on policies.

The EU societies are susceptible to these tactics due to a changing political landscape. Many EU states have witnessed a rise in right-wing populist parties. In 2022, Hungary's Fidesz party won the elections, making Viktor Orbán president. Similarly, in Sweden, the Sweden Democrats gained popularity in 2022. In Italy, the Brothers of Italy won the 2022 elections, while the PVV emerged victorious in the Netherlands in 2023.

In general, these right-wing political parties are questioning the legitimacy of political processes, both local as in the EU parliament. This creates division that affects political cohesion in the EU, which makes multilateral responses against Russia less effective. These political parties that are more aligned with Russian interests, limiting EU integration and NATO expansion.

Russia’s Influence in European Political Parties

Russia gained significant influence in political parties in the member states of the EU. According to Cohen and Radin, Russia has established connections with the far-right in Europe, exemplified by a gathering in St. Petersburg where far-right parties coordinated policy and criticized Western support for Ukraine (Cohen and Radin, 2019).

There is evidence that shows that Russia has ties with right-wing political parties. As an article “Putin’s friend” suggests, there are various political parties in the EU that are aligned with Russian interests and role in the EU (Wesslau, 2016).

The Economist referred to these political parties and individuals as useful idiots, a term was often used during the Cold War to describe non-communists regarded as susceptible to communist propaganda and psychological manipulation (The Economist, 2023).

The changing of the political landscape is significant for the effectiveness against Russian gray zone tactics aimed at the EU and its member states. A sharp divide between political opponents can polarize society on different topics like migration or further integration and expansion of the EU. When this division occurs, this can be exploited by disinformation campaigns to further the gap between political parties and render decision-making harder.

Use of AI in Disinformation Campaigns

Current strategies countering disinformation cannot withstand information technology developments. As research indicates, generative AI will become an enabler for disinformation campaigns. Makes current media literacy strategies less effective (Morris et al., 2019).

Generative AI can create synthetic digital content like images, text and audio, and video. This content distinction between real and fake information because it can be trained to mimic characteristics of people or organizations.

Furthermore, it can generate information at a larger scale trough advancement in automation and dissemination. Above all, Bayer et al. note the growing concern lies in the potential of deepfake text to manipulate public opinion by inundating recipients with algorithmically generated messages, leading to a distorted perception of political consensus (Bayer et al., 2021).

The EU parliament is concerned about the capabilities of generative AI. Recent advancements in large language models, such as OpenAI's ChatGPT, have the potential to greatly enhance foreign interference operations. One malign application of generative AI is deepfakes, which could erode trust in information and have significant implications for democracies (Caprile, 2023).

As we move forward, addressing disinformation campaigns and their evolving tactics remains a paramount concern for liberal democracies worldwide. It requires not only adaptability, but also international collaboration and a deep commitment to upholding democratic principles in an era where the battleground for hearts and minds has expanded into the digital realm.

Recommendations

I believe the EU must focus on societal resilience to counter the vulnerabilities in its liberal democratic states. There are several vulnerabilities in current strategies against Russian gray zone tactics in the information domain. I propose the following recommendations to create more resilient European society to counter the effects of Russia disinformation campaigns:

1. To promote effective rule of law within its member states, the European Union (EU) should respond proactively to rule of law issues observed in Hungary and Poland. It is recommended

that the EU applies pressure on these states through policy measures aimed at upholding the democratic processes and values outlined in the EU Copenhagen criteria. The EU can resort to diplomatic pressure, financial incentives, or conditional support as it did in the past. By doing so, the EU can ensure that its member states adhere to the principles of democracy, thus strengthening the overall rule of law framework within the Union. This recommendation is crucial for maintaining a harmonious and cooperative European community, where democratic principles are respected and protected.

2. The tension between censorship and self-regulation of online media must be acknowledged to ensure media pluralism, which is crucial for a functioning democracy. Censoring information can result in one-sided narratives and contribute to societal distrust. Therefore, it is recommended that social media platforms implement effective regulation measures, as demonstrated by Elon Musk's recent rule changes on X (formerly Twitter platform), despite the potential limitations.

3. The potential impact of generative AI, particularly in the form of large language models like ChatGPT, raises concerns about its role as a multiplier in information campaigns. The EU parliament acknowledges the exponential and uncertain effects of these AI developments on foreign interference operations. Furthermore, deepfakes may exacerbate a sense of general distrust, undermining the veracity of information and posing significant challenges for democracies. The EU should take actions that can take to mitigate these risks, such as investing in AI detection technology or collaborating with tech companies to develop safeguards.

Conclusion

In this chapter, I will reiterate the main points of this paper.

Gray Zone Tactics

The contemporary landscape of conflict has shifted from traditional warfare to more nuanced strategies, characterized by the leveraging of globalization and technological advancements, particularly in the information domain. While it is commonly believed that robust liberal democracies within Western EU nations are immune to such “gray zone” tactics, the reality presents a different picture. These tactics often operate discreetly, and their effects may not be immediately evident. In this context, it is essential to recognize that information campaigns wield a disruptive influence within the EU, comparable to their impact on weaker states at the EU's periphery, such as Poland and Hungary. The persistence of gray zone tactics is a result of the reduced likelihood of open conflicts between EU NATO and Russia.

Russian Tactics Employed

Russia has tactically employed the digital information space as its primary tool for exerting influence within the EU. This influence manifests aggressively during elections in stronger EU states and through propagandistic efforts in other EU nations, notably in the Baltic region. The overarching objective of Russia's strategy is to foster political discord and hinder European unity, specifically targeting NATO and EU integration and expansion.

EU's Current Strategy

The EU has recognized the menace posed by disinformation campaigns and has implemented a strategy centered on awareness, critical media literacy and regulations governing information platforms. In many respects, this strategy has proven effective.

Weaknesses in the Current Strategy

Vulnerabilities persist within the EU's current strategy. Firstly, the pressure on independent media outlets poses a significant concern. Instances of self-regulation and censorship, while intended to combat disinformation, run the risk of eroding trust within liberal societies. The potential consequences of stifling the free flow of information and limiting freedom of expression and opinions are substantial. Moreover, questions regarding the authority and independence of these censorship mechanisms make them susceptible to exploitation by Russia.

Secondly, shifts in the political landscape across many EU member states towards more nationalist viewpoints and reduced EU alignment pose a threat to the cohesion necessary for countering Russian influence. These changes in the political landscape create vulnerabilities that can be exploited through Russian gray zone tactics. This issue is closely intertwined with the pressures facing independent media.

Additionally, the infiltration of Russian influence within political parties in EU member states, such as the Netherlands, Germany, and France, diminishes the effectiveness of current strategies aimed at countering disinformation campaigns.

Lastly, advancements in technology, particularly in the realm of generative Artificial Intelligence, present new challenges for inoculation strategies and media literacy efforts, necessitating a reevaluation of the current approach.

Recommendations

Considering these weaknesses, I propose several recommendations to strengthen the EU's strategies against Russian disinformation campaigns:

Implementation of comprehensive critical media literacy programs across EU member states, recognizing that the digital information space is the primary medium for influencing both weaker and stronger EU nations.

Addressing the challenges presented by shifts in the EU's political landscape, particularly in nations where politicians are less aligned with EU values and more open to Russian influence, such as the Netherlands, Germany, and France.

By adopting these recommendations, the EU can enhance its resilience against Russian gray zone tactics within the information domain, ultimately fostering a more robust democratic society capable of withstanding such influences.

WORKS CITED

Bayer, Judit, Bernd Holznagel, Katarzyna Lubianiec, Adela Pintea, Josephine B Schmitt, Judit Szakács, and Erik Uszkiewicz. “Disinformation and Propaganda: Impact on the Functioning of the Rule of Law and Democratic Processes in the EU and Its Member States - 2021 Update,” 2021.

Bellingcat. “The GRU’s MH17 Disinformation Operations Part 1: The Bonanza Media Project,” 2020. https://www.bellingcat.com/news/uk-and-europe/2020/11/12/the-grus-mh17-disinformation-operations-part-1-the-bonanza-media-project/.

Belo, Dani. “Conflict in the Absence of War: A Comparative Analysis of China and Russia Engagement in Gray Zone Conflicts.” Canadian Foreign Policy Journal 26, no. 1 (January 2, 2020): 73–91. https://doi.org/10.1080/11926422.2019.1644358.

Berg, Elin, and Ulrica Pettersson. “Resilience and Resistance in the Digital Age: Revisiting the Threshold Effect in Total Defence,” 2022. https://doi.org/10.57767/JOBS_2022_0013.

Caprile, Anna. “Foreign Interference in EU Democratic Processes: Second Report,” 2023.

Carment, David, and Dani Belo. “Gray-Zone Conflict Management: Theory, Evidence, and Challenges.” Air University (AU), June 9, 2020. https://www.airuniversity.af.edu/JEMEAA/Display/Article/2213954/gray-zone-conflict-management-theory-evidence-and-challenges/https%3A%2F%2Fwww.airuniversity.af.edu%2FJEMEAA%2FDisplay%2FArticle%2F2213954%2Fgray-zone-conflict-management-theory-evidence-and-challenges%2F.

Carugati, Federica. “Democratic Stability: A Long View.” Annual Review of Political Science 23, no. 1 (May 11, 2020): 59–75. https://doi.org/10.1146/annurev-polisci-052918-012050.

Cohen, Raphael S., and Andrew Radin. Russia’s Hostile Measures in Europe: Understanding the Threat. Santa Monica, CA: RAND Corporation, 2019. https://doi.org/10.7249/RR1793.

Commissioner for Human Rights. “It is high time for Hungary to restore freedom of expression and media freedom - Commissioner for Human Rights - www.coe.int,” 2021. https://www.coe.int/az/web/commissioner/-/it-is-high-time-for-hungary-to-restore-journalistic-and-media-freedoms.

Gill, Ritu, Meghan Fitzpatrick, Matthew Duncan, and Anthony Seaboyer. “Coronavirus: Grayzone Tactics in Cyberspace,” 2020.

Gill, Ritu, and Rebecca Goolsby, eds. COVID-19 Disinformation: A Multi-National, Whole of Society Perspective. Advanced Sciences and Technologies for Security Applications. Cham: Springer International Publishing, 2022.

Issit, Micah. “Election Interference: Overview,” n.d.

Jensen, Benjamin. “The Cyber Character of Political Warfare,” 2017.

Kapoor, Nivedita. “Russia-EU Relations: The End of a Strategic Partnership.” Observer Research Foundation, Issue brief, no. 451 (2021).

Koninkrijksrelaties, Ministerie van Binnenlandse Zaken en. “Jaarverslag 2018 - Jaarverslagen - AIVD.” Onderwerp. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, April 2, 2019. https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2018.

Kreps, Sarah E. Social Media and International Relations. Cambridge Elements in International Relations. Cambridge New York Port Melbourne New Delhi Singapore: Cambridge University Press, 2020.

Kuczyńska-Zonik, Aleksandra. “Russian Propaganda: Methods of Influence in the Baltic States,” 2021.

Meister, Stefan. “NATO Review - The ‘Lisa Case’: Germany as a Target of Russian Disinformation.” NATO Review, July 25, 2016. https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html.

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe. Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War. Santa Monica, CA: RAND Corporation, 2019. https://doi.org/10.7249/RR2942.

Pettyjohn, Stacie, and Becca Wasser. Competing in the Gray Zone: Russian Tactics and Western Responses. RAND Corporation, 2019. https://doi.org/10.7249/RR2791.

“Poland: Attacks on Media Freedom and the EU Legal Order Need to Stop | News | European Parliament,” September 16, 2021. https://www.europarl.europa.eu/news/en/press-room/20210910IPR11928/poland-attacks-on-media-freedom-and-the-eu-legal-order-need-to-stop.

Roozenbeek, Jon, Sander van der Linden, Beth Goldberg, Steve Rathje, and Stephan Lewandowsky. “Psychological Inoculation Improves Resilience against Misinformation on Social Media.” Science Advances 8, no. 34 (2020): eabo6254. https://doi.org/10.1126/sciadv.abo6254.

Stelzenmüller, Constanze. “The Impact of Russian Interference on Germany’s 2017 Elections.” Brookings, 2017. https://www.brookings.edu/articles/the-impact-of-russian-interference-on-germanys-2017-elections/.

“Texts Adopted - Foreign Interference in All Democratic Processes in the European Union, Including Disinformation - Thursday, 1 June 2023.” Accessed December 2, 2023. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0219_EN.html.

The Economist. “Vladimir Putin’s Useful Idiots.” 2023. https://www.economist.com/europe/2023/07/03/vladimir-putins-useful-idiots.

Vilmer, Jean-Baptiste Jeangene, and Heather Conley. “Successfully Countering Russian Electoral Interference: 15 Lessons Learned from the Macron Leaks,” 2018, 6.

Wesslau, Fredrik. “Putin’s Friends in Europe.” ECFR, October 19, 2016. https://ecfr.eu/article/commentary_putins_friends_in_europe7153/.

ABOUT THE AUTHOR

Leon Wiskie is a Dutch cybersecurity professional. His work focuses on cybersecurity and information security strategy in large commercial and governmental organizations. He has over 20 years of professional experience in various organizations in the Netherlands. He is also a part-time graduate student pursuing a Master's degree in International Relations at Webster University, Leiden Campus. His research interests are international security, national security, and the intersection of cybersecurity and information technology, including artificial intelligence, information warfare and autonomous systems. Leon holds a Master's degree in Business Informatics from NCOI University of Applied Sciences and a Master's degree in Cybersecurity Engineering from The Hague University of Applied Sciences in the Netherlands.

ABOUT THE GLOBAL POLICY HORIZONS RESEARCH LAB

Webster University's Global Policy Horizons Lab is a policy-focused research entity where students, Lab researchers, affiliated faculty, as well as members of the policy community from across disciplines, can explore national and global security issues, generate original research, as well as produce peer-reviewed policy papers and commentaries. The Lab pursues innovative research focusing on unconventional threats, identity and security, role of technology in security, economic security, as well environmental and food security. The goal of the Lab is to become a knowledge hub that informs national governments and other members of the global policy community on contemporary and future security challenges.

The current Director of the Lab is Professor Dani Belo, PhD.