Russian Information Warfare in the European Union

Clarke, Jesse

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Clarke, J. (2022). Russian Information Warfare in the European Union. *Russian Analytical Digest*, 282, 13-16. https://doi.org/10.3929/ethz-b-000541999

ANALYSIS

Russian Information Warfare in the European Union

By Jesse Clarke, George Washington University

DOI: 10.3929/ethz-b-000541999

Abstract:
The European Union is one of Russia's prime subjects in the modern information war. Russia targets the EU using both covert and overt disinformation methods, while thematically focusing on divisive topics like member state sovereignty and the COVID-19 pandemic. Compared to other international actors, the EU's policy response has been relatively robust, focusing on increasing its populace's media literacy and working with tech companies to regulate disinformation on their platforms. Although ahead of many others, coordination and implementation issues inherent to the EU's structure have limited its ability to counter Russian disinformation in certain areas. This article aims to use the EU as a case study to contribute to the literature around viable policy options for combating Russian information warfare operations.

Long in the Crosshairs

The European Union (EU) has long been a target of Russian information warfare. From the time of Peter the Great, through Joseph Stalin, and now Vladimir Putin, Russia and its leaders have sought to influence how Europeans view their neighbors to the east. In a modern context, Russia's resurgence in the last decade as an actor hostile to the West has coincided with a dramatic uptick in disinformation operations in Europe meant to justify Russia's actions and provide viewpoints sympathetic to them. Representing over 60% of Europe's population and counting three former Soviet Republics and six former Warsaw Pact states among its members, the EU is uniquely situated to be a target of Russian information warfare. Thematically, much of Russia's information operations in Europe follow trends from elsewhere in regard to the overall desire to sow discord and division, although there are a few key differences. Additionally, the EU's close proximity to Russia and its supranational nature make it an important case study for global actors seeking to counter Russian disinformation. By analyzing the unique aspects of Russian information warfare in the EU, followed by the successes and failures of the EU's responses, some potentially viable policy options to counter Kremlin-based information operations can be illuminated.

How the EU is Being Targeted

As in many other locations, Russian information warfare toward the EU is both covert (i.e., the source is not known) and overt (the source is known). It is important to draw a distinction between these two methods, as they can vary drastically in both their approaches and their subject matter. Overt Russian disinformation in the EU mainly comes in the form of state-sanctioned propaganda originating from the Kremlin. It emanates largely from two predominantly English-speaking, state-owned media outlets—RT and Sputnik News—that Russia uses to spread narratives favorable to its government and contribute to the overall information battle. RT and Sputnik use both cable and satellite to propagate their messages, but their audience in the EU and abroad is mainly reached through social media (Golovchenko, 2020). However, following Russia's invasion of Ukraine in February 2022, the EU issued a blanket ban in early March on RT and Sputnik and stated that any outlets that continue to publish their content will be subject to fines. A few days earlier, tech giants like Facebook and YouTube had begun to restrict access to these channels on their platforms in Europe in retaliation for the invasion. Following these measures, it is unclear what impact Russian overt disinformation will have on the EU in the future; it is likely that the Kremlin will focus on covert methods going forward.

Russia's use of covert disinformation campaigns in the EU is much more difficult to track due to its secretive nature and the associated attribution challenges. The primary method focused on in the scholarly literature is Russia's use of fake accounts on Western social media, specifically Twitter (Golovchenko, 2020). These can take the form of "automated accounts, fake profiles, bots or 'army of trolls'" and have "the advantages of low cost, rapid spread and high impact" (Durach, 2020, p. 6). In the early 2010s, much of this covert information warfare took the form of purely fabricated stories, or "fake news," designed to either sow discord or promote a particular pro-Russian narrative. After many European governments adopted policies to combat fake news and invested in media literacy programs, however, social media companies started to regulate false content more stringently (Durach, 2020; Sarwein, 2020). This trend has caused some scholars to speculate that covert disinformation campaigns in the EU are moving toward selective amplification of real, often polar-

izing, news stories in place of the traditional fake news model (Sarwein, 2020).

The Themes of Disinformation

Thematically, Russian information warfare can vary greatly depending on its intended recipient, but many scholars have noted the foundational similarity of an attempt to "sow confusion, doubt, and to blur the boundaries between enemy and non-enemy, war and peace, in order to make the population question who is the enemy and whether they are at war" (Golovchenko, 2020, p. 4). Nevertheless, in the case of the EU, there are a few unique characteristics of Russian disinformation that are worth noting.

One common thread is efforts to push for self-determination and sovereignty among citizens of EU countries and, correspondingly, against EU centralization, in a narrative that depicts Brussels as a group of distant bureaucrats (Magdin, 2020). This takes the form of promoting nativist and nationalist sentiments, notably in European countries with deep pre-existing divisions (Spain, Belgium) or with historically shifting borders (Western Ukraine–Poland, Finland–Sweden, Transylvania–Hungary). In former Eastern Bloc countries like Romania and Poland, disinformation can also hark back to the communist era by playing on nostalgia and, in the case of Romania, highlighting the economic struggles brought about by adopting the EU's monetary model (Magdin, 2020). These narratives contribute to the anti-Western views that Russia seeks to embolden, while also attempting to rehabilitate Russian soft power in Eastern Europe by arguing that life was better for the average citizen under the Russia-led Soviet Union. Paradoxically, there has recently been an increase in Russian disinformation campaigns in support of discussions around EU "strategic autonomy," or the idea that the EU should take steps to create its own military capabilities in order to be less reliant on NATO. This is largely seen by scholars as a geopolitical attempt to undermine U.S. and NATO influence in Europe (Magdin, 2020). Anti-Western narratives are also seen in Russian information warfare surrounding the COVID-19 pandemic and vaccinations. Russia sought to improve its image by "comparing [its] handling of the pandemic to how Western governments have been handling it, in some cases by falsely representing the actions of the EU and its member states" (Pamment, 2020, p. 11). The efficacy of Western vaccines was also repeatedly questioned by disinformation campaigns in order to make Russia's Sputnik-V vaccine seem more effective by comparison.

How the EU is Responding

Compared to other actors impacted by Russian information warfare, the EU's response has been relatively strong. However, there are still a few key structural factors that limit the EU's overall success in combating disinformation campaigns.

Substantive EU policy on information warfare was first adopted as a reaction to the Russian annexation of Crimea in 2014 (Pamment, 2020). The annexation came in tandem with a barrage of disinformation campaigns on social media to garner support for the Kremlin's actions, and the EU perceived the Russian threat to be one worth addressing seriously. The EU's European External Action Service (EEAS) was the natural home for a new policy to address information warfare, as its Strategic Communications arm already housed two divisions related to the subject: the Communications Policy and Public Diplomacy division, which mainly "manages communications campaigns, internal communication, social media accounts, and digital platforms as well as public and cultural diplomacy," (Pamment, 2020), and the Task Forces and Information Analysis division, which provides analytical support for communications policies and focuses largely on southern and eastern Europe. At the time, neither of these divisions were adequately equipped to handle the threat of Russian information warfare. Thus, the East StratCom Task Force was created by the European Commission in 2015 specifically to "identify and expose Russia's disinformation campaigns" (Durach, 2020, p. 9). StratCom produces a weekly report flagging pro-Kremlin disinformation on its EUvsDisinfo website, and at the time of writing had an open-source database of over 13,000 examples of Russian disinformation ("EUvsDisinfo", 2022).

Given that many disinformation campaigns take place on social media websites, the EU has found it necessary to collaborate with private industry on some of its policies to counter Russian information warfare. When it comes to private companies and information warfare, some argue that it is best for corporations to self-regulate, while others claim that corporations cannot be trusted and that content on their platforms should be directly regulated by the state. The EU has opted for something in between, aptly titled "co-regulation" (Durach, 2020). The goal of this strategy is to bridge the public-private gap by finding "a compromise which allows the implementation of a series of measures by the internet platform companies, monitored by an authority" (Durach, 2020, pp. 9–10). In this vein, the EU created in October 2018 its Code of Practice on Disinformation, which is meant to serve as a guide of sorts for private companies regarding how they should regulate their platforms. Companies signed on to monitor five areas related to disinformation: online advertisements, political advertising, integrity of services, transparency for consumers, and transparency for researchers ("EU Code of Practice", 2018), however this policy has been criticized because

companies self-report their progress rather than it being externally reviewed, leading to questions of efficacy. This highlights the importance of addressing the challenges brought about by the private sector's necessary role in adopting policy to counter disinformation.

A few months after the Code of Practice was introduced, the EU announced its Action Plan Against Disinformation in December 2018. This plan was structured around four key pillars: "improving the capabilities of Union institutions to detect, analyse and expose disinformation, strengthening coordinated and joint responses to disinformation, mobilising private sector to tackle disinformation, raising awareness and improving societal resilience" ("Action Plan Against Disinformation", 2018). The action plan also highlighted the need for East StratCom's mandate to be expanded and its funding increased, as well as calling for initiatives in the realms of media literacy and journalism (Pamment, 2020). Notably, the creation of a Rapid Alert System to detect disinformation threats and improve information-sharing was also proposed. This idea came to fruition in March 2019; the resulting system was "intended to connect to existing real-time monitoring capabilities inside and outside of the EU, such as the Emergency Response Coordination Centre and the EEAS Situation Room, as well as the G7 Rapid Response Mechanism and the North Atlantic Treaty Organization (NATO)" (Pamment, 2020, p. 9). While a useful tool in theory, the Rapid Alert System has unfortunately not lived up to its potential thus far. This is a result of the EU's largely decentralized nature, as it is up to individual member states to decide when and how to share information through the Rapid Alert System, and definitions of—and importance given to—Russian disinformation can vary wildly depending on the politics of the country. While effective for small coalitions of member states passionate about opposing disinformation, it has struggled to break through on a pan-EU level due to low engagement. This is indicative of a problem that plagues the EU across many of its policy areas related to information warfare, namely coordination and implementation (Saurwein, 2020). However, this may well change in the future, as the Russian invasion of Ukraine has united Europe against Russia in a way not seen in decades.

Conclusion

Overall, EU policy to combat Russian information warfare has been much more substantial and targeted than that of many other actors. The EU has benefited from a relatively early response to disinformation campaigns and has had time to refine its program. Its successes in this field have largely been based on clarity of mission, as well as transparency with its populace. Unlike other actors, the EU has not sought to mount counter-offensives in the realm of information warfare, but instead seeks to promote awareness of Russian efforts through media literacy programs and EEAS plans of action. Additionally, the EU has attempted to work alongside private companies through its co-regulation model to tackle disinformation.

However, the EU has necessarily been limited by problems of implementation and coordination. While it is easy for the EU to announce a useful policy like the Rapid Alert System, it is much harder to put it into practice due to the differing opinions of individual member states and the EU's inability to force them to comply. In any case, its model of decisive action centered around public awareness offers a helpful policy option for other actors seeking to combat Russian information warfare, while the clear gaps in its policy could be addressed if adopted by an actor with a stronger federal mandate.

About the Author

Jesse Clarke is a graduate student at International Affairs at George Washington University, concentrating on international security studies in Europe. He received his Bachelor of Arts in Political Science and International Studies from the University of Oregon in 2020.

Bibliography

- "EU Code of Practice on Disinformation," European Commission, September 26, 2018, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.
- "EUvsDisinfo," European Union East StratCom Task Force, https://euvsdisinfo.eu.
- Fabrizio Di Mascio et al. (2021) Covid-19 and the Information Crisis of Liberal Democracies: Insights from Anti-Disinformation Action in Italy and EU. *Partecipazione e conflitto*. 14 (1), 221–240.
- Flavia Durach et al. (2020) Tackling Disinformation: EU Regulation of the Digital Space. *Romanian journal of European affairs*. 20 (1), 5–20.
- Golovchenko, Y. (2020) Measuring the scope of pro-Kremlin disinformation on Twitter. *Humanities & social sciences communications*. 7 (1), 1–11.
- High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan Against Disinformation," 1.

- Pamment, J., 2020. *The EU's role in fighting disinformation: taking back the initiative* (Vol. 15). Carnegie Endowment for International Peace.
- Radu Magdin (2020) Disinformation campaigns in the European Union: Lessons learned from the 2019 European Elections and 2020 Covid-19 infodemic in Romania. *Romanian journal of European affairs*. 20 (2), 49–61.
- Saurwein, F. & Spencer-Smith, C. (2020) Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe. *Digital journalism*. 8 (6), 820–841.
- Wagnsson, C. & Hellman, M. (2018) Normative Power Europe Caving In? EU under Pressure of Russian Information Warfare: Normative Power Europe Caving In? *Journal of common market studies*. 56 (5), 1161–1177.

ANALYSIS

Russian Information Warfare: Policy Recommendations

By Jesse Clarke, Jacqueline Evans, Jessica Brzeski, and Nash Miller (all George Washington University)

DOI: 10.3929/ethz-b-000541999

Abstract

This final article on Russian information warfare presents policy recommendations that can be adopted to combat and respond to information warfare. Each case study exhibits unique circumstances that illuminate potential policy options for counteracting Russian disinformation campaigns. After analyzing both the successes and failures in each case study, the following policy recommendations emerged: transparency, preemptive information-sharing, media literacy campaigns, private-sector engagement, and multilateral cooperation. These policy recommendations provide a broad framework for all countries facing a similar threat.

Introduction

Russian information warfare is an existential threat to liberal democracies that value peace, stability, and the rule of law. Due to the widespread, global nature of Russia's information operations, countries worldwide have been impacted by these campaigns. Depending on the target, distinct circumstances can dramatically alter the way that Russian disinformation manifests itself. However, in analyzing four case studies of actors that have been especially impacted by information warfare—namely Ukraine, Poland, the United States, and the European Union—recurring themes of what has (and has not) been successful in countering the Kremlin emerged. Among the most notable are: transparency, preemptive information-sharing, media literacy campaigns, private-sector engagement, and multilateral cooperation. Due to their success in widely varied contexts, these policy options can hopefully serve as tools for any potential actor looking to counter Russian information warfare now and in the future.

Transparency

The first policy that all governments, institutions, and agencies should adopt is transparency. One of Russia's goals is to weaken society by creating division and doubt about what is true and what is false. This is particularly evident when you examine how Russia has used information warfare to make average citizens question the legitimacy of their own governments and the information that they receive from them. Although a vital part of democracy is the freedom to question the information of a government, Russia has exploited this to foment division and make people doubt the very legitimacy of their own governments and whether they truly support the rule of law.

The best way to combat these efforts is by being transparent with the public, providing factual evidence that backs up an official government claim. The United States has attempted this strategy through its intelligence community's bid to shine a light on Russian disinformation campaigns in advance of the February 2022 invasion of Ukraine, sometimes before the events had even happened. Although met with uncertainty at first, when many of these events eventually transpired, this strategy proved itself an effective tool for transparency.

The European Union also seeks to be transparent with its populace by tracking and exposing examples of Russian disinformation on its website EUvsDisinfo, which currently has a database of over 13,000 cases. The EU emphasizes the explanatory rather than inflamma-