Russian Information Warfare: Policy Recommendations

Clarke, Jesse; Evans, Jacqueline; Brzeski, Jessica; Miller, Nash

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Clarke, J., Evans, J., Brzeski, J., & Miller, N. (2022). Russian Information Warfare: Policy Recommendations. *Russian Analytical Digest*, 282, 16-18. https://doi.org/10.3929/ethz-b-000541999

- 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-

tory nature of EuvsDisinfo, which is run by the body's East StratCom Task Force. The EU values transparency and public awareness of disinformation above all else, and the organization publicly states on its website that no counter-information operations are conducted.

Information warfare is inherently based on lies, deception, and misdirection. For this reason, policy intended to counter it should focus on being as transparent as possible with the public in order to cut through the fog and build trust among citizens.

Preemptive Information-Sharing

Another policy option that has thus far shown promising results in combating Russian information warfare is the use of preemptive information-sharing. This policy option calls upon members of the government and intelligence community to preemptively release information to the public once the intelligence agencies are warned of a particular misinformation or disinformation campaign that Russia is planning to implement. Preemptively warning about an upcoming Russian information operation alerts both the general public and foreign countries ahead of time, thus enabling them to prepare for and weaken Russia's operation.

Currently, this strategy is successfully being implemented by the US in regard to Russia's invasion and the Kremlin's response to the global sanctions. Two key examples that demonstrate its overall success include the US releasing intelligence that Russia was planning to use a false flag operation to justify the invasion and President Biden's warning to American corporations that Russia was going to disrupt the US via a hacking campaign. In both cases, the policy of preemptive information-sharing informed the relevant parties and the public of the Kremlin's antics, thus reducing the attack's likelihood of success and giving actors time to steel themselves against it.

Other countries and multilateral organizations should employ this policy, as it essentially beats Russia at its own game. By releasing reports that Russia intends to carry out a misinformation or disinformation attack, it makes the public aware of the threat, thereby making information warfare less effective because individuals in society are less likely to fall victim to the false narrative and propaganda slogans.

Media Literacy Education

Campaigns to promote media literacy can be a potent force in inoculating audiences against information warfare. If given the proper intellectual tools, audiences can be taught to identify misinformation, independently fact-check, and compile trustworthy verified sources.

Latvia, which has been on the front line of Russian information warfare for years, has successfully used media literacy education at schools and universities. Similarly, since the annexation of Crimea and invasion of the Donbass in 2014, Ukrainian civil society groups have successfully implemented a number of programs aimed at improving media literacy.

Universities, schools, and other organizations can conduct short courses or workshops for students, journalists, and political activists to effectively recognize misinformation. Civil society groups and journalist organizations have also found success in exposing and disproving Russian misinformation using verifiable facts. Openly exposing misinformation narratives can drown out and delegitimize information warfare campaigns, and can be an effective alternative to censorship, which raises civil liberties concerns.

As governments scramble to protect their populations from information warfare, media literacy education campaigns—starting from an early age and conducted by balanced and trusted organizations—can have a major impact.

Private-Sector Engagement

Engagement with the private sector has shown itself to be a crucial aspect of countering Russian information warfare. Since many covert disinformation campaigns are conducted via social media, the corporations that run these websites and apps necessarily have a role to play in coordinating responses to this threat. There are many schools of thought on how the public and private sector should interact within this space, with some arguing that the public sector should simply dictate policy to corporations and others advocating for allowing companies to self-regulate their content.

The European Union has opted for something in between, called co-regulation, and this model serves as a useful example for how states may approach policy to counter information warfare in a pragmatic way. The co-regulation model seeks to find areas of potential cooperation with social media companies in a way that aims to foster goodwill and keep them on the side of governments in the fight against disinformation. The EU has attempted to implement this through its Code of Practice, which serves as a guide for how private companies should regulate disinformation in key areas such as political advertising and general integrity of services.

The Code of Practice is far from perfect: critics have noted that the progress companies make in tracking disinformation areas is largely self-reported and is not subject to strict enforcement. However, it provides a helpful framework for how states and international actors can orient policy against disinformation in a way that includes the private sector. Large social media companies must be considered in any attempt to counter Russian information warfare due to how heavily the

Kremlin relies on these media to conduct its information operations. Many of these companies have a vested interest in regulating disinformation, but their concerns are primarily financial and are not inherently opposed to the idea of Russian-originated accounts stoking divisive topics on their platforms. Policies that bring the private sector into the fold as a collaborator against disinformation, like the EU's Code of Practice, are preferable to allowing corporations to be the sole arbiters of what should and should not be allowed on their platforms.

Multilateral Cooperation

The scope of information warfare has evolved beyond the borders of one country, with impacts spreading globally. Therefore, for a country to effectively combat information warfare of any type, a multilateral effort must be considered. This entails countries coming together in creating effective solutions to combat information warfare by implementing standards and structures through shared experiences. Not only does multilateral cooperation to combat information warfare strengthen efforts, but it also holds countries accountable in their own domestic processes. Overall, countries should make multilateral cooperation one of their key solutions to combating information warfare

In the case of Poland, binding obligations to multilateral security measures within the EU and NATO have strengthened domestic information security structures. These include physical and legal implementations that help combat impending threats and destruction caused by Russian information warfare. A desire to measure up to the legal standards of the EU and NATO has not only impelled the initiatives taken by Poland in the security realm, but also inspired domestic enterprise. In addition, as a member state of both organizations, Poland has also contributed to their information security. Therefore, a multilateral approach to Russian information warfare fosters greater accountability and ingenuity in combating the various associated threats.

Multilateral cooperation in the face of information warfare will resolve a variety of issues when it comes to combating this evolving threat. As globalization has spread, so too have the platforms and techniques of information warfare evolved to impact a series of actors ranging from online citizens to government institutions. The case study of Poland perfectly exemplifies why multilateral cooperation would benefit countries as they attempt to counteract the various derivative threats of information warfare. An approach that seeks multilateral cooperation would strengthen the legal and physical structures of countries while implementing domestic accountability. Of course, multilateral cooperation is not a perfect solution, but it offers a pre-established platform that would provide the basis for further problem solving.

Conclusion

As demonstrated in this series of articles, Russian information warfare poses a massive threat to the future of democracy. The danger lies in the Kremlin's ability to use various methods and tools that target each nation differently, thus making a global response more difficult. That said, as laid out in the previous sections, the successes and failures of democracies around the world show which countermeasures work and, therefore, what policies should be adopted to limit Putin's ability to further divide the democratic world. By adopting transparency, preemptive information-sharing, media literacy campaigns, private-sector engagement, and multilateral cooperation, countries can combat information warfare while protecting vital civil liberties. Information warfare is here to stay and will continue to evolve as social media and the internet continue to change. Thus, states must develop strong responses now and prepare for future threats.

About the Authors

The authors are all pursuing MA degrees in international affairs at the George Washington University's Elliott School of International Affairs.

Acknowledgement

We would like to thank Robert Orttung of the George Washington University for all of his support and advice throughout this project. Additionally, we would like to thank the George Washington University for providing funding for our group to travel to Warsaw and Krakow in order to interview experts in Poland about the Polish and Ukrainian responses. Finally, to all of the people we have interviewed, thank you so much for your time and fascinating insights.