Countering Russian Disinformation

JOSEPH W. ROBBINS

Executive Summary

Disinformation is a tool commonly used by a number of states to sow discord, undermine faith in governing institutions, stoke fear and anxiety, and ultimately achieve certain policy goals. Over the past several years, Russia, its government agencies, and affiliated groups have used a combination of social media savvy and disinformation strategies to further Russian influence largely by weakening its foes. This use of disinformation to weaken the North Atlantic Treaty Organization (NATO), cast doubt on the European Union, and undermine countries throughout the world has prompted countries to develop countermeasures to stymy these efforts. The Czech Republic and Estonia are two such countries that have developed amalgamated approaches to stifle Russian subversive attempts. The Czech and Estonian responses are explored and offered as robust solutions to this growing threat.

Introduction

Russian disinformation operations are currently a cornerstone of the country's efforts to wield influence worldwide. Whether trying to weaken the European Union, NATO, individual countries, or other groups, Russian operations perpetrated by cyberespionage groups such as Cozy Bear or Fancy Bear have fostered much anxiety, fear, and division throughout the world. Disinformation efforts have their roots in "active measures" or propaganda efforts orchestrated by the Soviet Union. Yet, the key difference here is that contemporary Russian efforts have been more successful than any Soviet operation could have ever imagined due to rethinking communication strategies (elaborated below) and the use of social media technology. Indeed, Russian disinformation operations were credited with sowing discontent in the United States and curtailing Hillary Clinton's electoral support in 2016, boosting support for far-right Italian political parties among those consuming alternative news stories in 2018, and prompting a decline in Spanish leaders' ability to influence public opinion during the 2017 Catalan crisis.[115]

Modern Russian propaganda efforts have led to policy responses from multilateral organizations,

115. Veronika Špalková, *Influence of Russian Disinformation Operations: Specific Examples in Data and Numbers* (Prague: Kremlin Watch Program, 2019), https://www.europeanvalues.net/wp-content/uploads/2019/02/Influence-of-Russian-Disinformation-Operations-Specific-examples-in-data-and-numbers.pdf.

national governments, social groups, and corporations. A number of these approaches have been adopted by the Czech Republic and Estonia. The extent to which they will be successful over time is unclear, particularly given the Czech Republic President Miloš Zeman's pro-Russia inclinations along with Estonia's burgeoning populist presence, both of which play right into Moscow's hands. Nonetheless, these approaches show a determination to combat disinformation threats that is rarely seen elsewhere. For example, in the United States, the response to disinformation currently largely rests on corporate policies set by Facebook, Twitter, and YouTube. In places like the Czech Republic and Estonia, moving beyond dependence on corporate response alone is thus far proving to be a more effective response to thwart Russian efforts.

Russian Disinformation Strategies

Internet-aided Russian disinformation strategies have been a hallmark of the country's destabilization efforts for the past several years. Disinformation, for the purposes of this article, refers to the creation or spreading of information that is misleading or false with the intention to manipulate a given audience. Democracies, anchored in the embrace of a free press, are particularly vulnerable to disinformation, although this tactic has been used in many different settings. To date, Moscow has used these tools to target Ukraine, Germany, Italy, Syria, Spain, the United Kingdom, NATO, the European Union, and the United States.

The playbook used in these countries contains a variety of actions undertaken by various actors—not all governmental entities. Research by Watts and by Weisburd, Watts, and Berger summarizes the complex approach well.[116] The overall approach unfolds in multiple stages and begins by actors infiltrating an audience then influencing it, followed by using *kompromat* to drive damaging narratives against certain politicians, movements, or organizations. These stages are administered through a combination of media actors (e.g., Russia Today [RT], Sputnik, and the country's Internet Research Agency [IRA]), intelligence agencies (GRU, FSB, and SVR), along with "troll factories," hackers, and "honeypots." As Weisburd, Watts, and Berger explain, these groups work hand-in-hand such that "trolls sow doubt, the honeypots win trust, and hackers . . . exploit clicks on dubious links sent out by the first two."[117] Mark Galeotti lays out a helpful schematic of the various forces and actors involved in Russian disinformation campaigns, each relating to the Kremlin in a different way.[118] The end result of Russia's technological "active measures" is a multichanneled, highly active, relentless propaganda machine that has pumped out a tremendous amount of damaging information in multiple contexts.

Russian disinformation has proven to be effective in large part because it is motivated by a fundamental shift in communication strategies. Russian disinformation efforts have been influential because they seek to form an early narrative, repeat the narrative, and employ a wide range of outlets, channels, and users to parrot this narrative.[119] Because these Kremlin-engineered narratives

116. Clint Watts, *Messing with the Enemy*, (New York: HarperCollins, 2018); Andrew Weisburd, Clint Watts, and JM Berger, "Trolling for Trump: How Russia is Trying to Destroy Our Democracy," War on the Rocks, November 6, 2016, https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.

117. Weisburd, Watts, and Berger, "Trolling for Trump."

118. Mark Galeotti, *Controlling Chaos: How Russia managers its political war in Europe* (Lond.n: European Council on Foreign Relations, 2017), https://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe.

119. Christopher Paul and Miriam Matthews, *The Russian 'Firehose of Falsehood' Propaganda Mode* (Santa Monica, CA: RAND Corporation, 2016), https://www.rand.org/pubs/perspectives/PE198.html.

are often the first of their kind (although some sources are indigenous in the target country, which the Kremlin then amplifies), the target audience has no frame in place to counter or challenge this new information. Likewise, the narratives are repeated and echoed by numerous actors, giving them the appearance of credible information. Indeed, from the public's perspective, multiple actors with different perspectives reaching the same conclusion gives a narrative the veneer of truth.[120] With Russian troll farms operating 24 hours a day, it is easy to see how these campaigns author new narratives and disseminate them widely and frequently. This approach essentially overwhelms the social media user with the amount of repetition and leads them to either accept the disinformation as fact or to fall back on their own baseline biases.

Responding to these disinformation campaigns is very difficult, particularly in democracies that are buoyed by the free press. There has been great variance in how democracies and organizations like the European Union have responded to these efforts, with varying degrees of success.[121] This article examines the approaches used by the Czech Republic and Estonia along with multilateral responses from both the European Union and NATO. The approaches discussed here are still evolving but it is increasingly clear that to have success against Russian disinformation and this complex propaganda machine, a multifaceted approach is vitally important.

Czech Responses

The Czech Republic is one of Europe's leaders in combatting Russian disinformation. The country's government agencies are leveraged to respond to these attacks, including a specifically designed agency, the Center Against Terrorism and Hybrid Threats (CTHT). Its work is enhanced by the Czech Security Information Service (*Bezpečnostní informační služba,* or BIS), civil society group mobilization, and research from think tanks.

The Czech Republic's efforts are notable in their ingenuity but also because they have been in place despite strong political headwinds: Czech political leaders feature some notable pro-Russian political officials.[122] President Milos Zeman is often viewed as one of the Kremlin's most visible allies in Europe. Zeman has supported terminating Russian sanctions, is friends with oligarch Vladimir Yakunin, and has advisors with reportedly close ties to Russian interests. Then there is the legislature, where Russian support includes forces on the left and the right. The Czech Chamber of Deputies 2017 election witnessed over 20 percent of the vote going to parties often espousing stances in line with Russian narratives (e.g., anti-NATO, Euroskepticism) such as the far-right Freedom and Direct Democracy Party (SPD, which received 11 percent) and the Communist Party of Bohemia and Moravia (KSČM, which received 8 percent).

Despite this political landscape, the country's government has put in place a multifaceted strategy to respond to these external threats. The country's overall orientation stems from its insistence that

120. Ibid.

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

122. Heather Conley, Donatienne Ruy, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook 2: The Enablers* (Washington, DC: CSIS, 2019), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Conley_KPII_interior_v3_CzechRepublic.pdf.

Russia, like other countries, respect international law and the territorial integrity of other states.[123] This stance was naturally insufficient to discourage Russia's efforts to spy on, hack, and sow discord in the Czech Republic. Consequently, the country's Security Information Service has been at the forefront of monitoring state-sponsored propaganda targeting Czech society. Intelligence agencies have sought to name and shame attackers and to raise awareness of cyberattacks. The government also created the CTHT, an analytical body within the Ministry of the Interior with access to classified information that is charged with reviewing disinformation, preparing policy proposals, and working with other government agencies and outside organizations to raise awareness of the agency's findings and collaborate to resist these intrusions. The CTHT is also focused on proactive measures, such as planning for election-related attacks and mitigating vulnerabilities.

The Czech government closely studied the communication strategy undergirding Russian disinformation efforts to develop the country's response. Czech think tanks and civil society have played an important role in countering frequent repetition of various narratives or the seemingly widespread embrace of these stances. Russian messaging on domestic policy often embraces Islamophobic, anti-immigration, corruption allegations, or certain Czech leaders' purported ties with the Secret Police, while foreign policy messaging often advances claims that the United States is out to control the world or that the European Union and NATO are the aggressors throughout Europe. Czech civil society has engaged in both fact-checking to identify false or unfounded claims and investigative journalism, which can "out" or counter trolls online and counter chain emails that are commonplace in the Czech Republic.[124] These efforts are buttressed by direct action via People in Need's One World program, which promotes critical thinking, information literacy, and curriculum in primary and secondary schools to foster a more resilient and news- and digitally-literate population.[125] The educational front is supported by efforts from researchers and curriculum through Masaryk University and Charles University.

Think tanks have been active participants in the struggle against disinformation as well. The European Values Center (EVC) and the Prague Security Studies Institute (PSSI) have been at the forefront of this movement.[126] The EVC established its Kremlin Watch Program in 2015, which highlights disinformation campaigns throughout Europe.[127] It also reviews countermeasures used across the continent and evaluates their effectiveness. The EVC works with Czech agencies involved in combatting subversive Russian influence (e.g., Ministry of the Interior). Similarly, the PSSI has sought to spread the word on tactics used by the Kremlin and to develop policy proposals to help Prague better respond to these external threats. While this organization focuses on an array of security threats, such as economic, space, energy, and transnational, its work in the realm of cyber threats is particularly notable as it has orchestrated initiatives to focus on disinformation targeting parliamentary and

123. Mariam Tsitsikashvili, *Comparing Lessons Learned from Countering Russian Disinformation in Georgia and the Czech Republic* (Prague: Kremlin Watch Program, 2019), 10, https://www.kremlinwatch.eu/userfiles/comparing-lessons-learned-from-countering-russian-disinformation-in-georgia-and-the-czech-republic.pdf.

124. Ibid.

125. Ibid., 12.

126. "Aims and Purposes," European Values, https://www.europeanvalues.net/o-nas/nase-poslani/; "About us," Prague Security Studies Institute, http://pssi.cz/.

127. "About Kremlin Watch," Kremlin Watch, https://www.kremlinwatch.eu/#about-us.

presidential elections. For example, PSSI has partnered with the International Republican Institute (IRI) to carefully analyze election-related news stories posted on disinformation sites.[128]

Estonian Responses

Estonia's political space—and society in general—is markedly different from the Czech Republic's. Estonia's ethnically Russian population is much larger (nearly 25 percent of the population) than the Czech Republic's (estimated at around less than 1 percent). President Kersti Kaljulaid has a style and political leanings that stand in stark contrast to Milos Zeman's. Although Prime Minister Jüri Ratas's Center Party (*Eesti Keskerakond*) is the preferred party among Russian-speaking Estonians, the center-right Reform Party (*Eesti Reformierakond*) became the largest party after the 2019 Riigikogu elections, winning 29 percent of the vote. Nevertheless, after the Reform Party's coalition bid fell short of the necessary votes, Ratas's Center Party obtained the votes necessary to secure a coalition with the Conservative People's Party (a far-right populist party) and Isamaa (a Christian Democratic, center-right party). Yet Estonia's leadership has adopted a determined stance vis-à-vis Russia. Ratas's government has pushed to maintain sanctions on Russia, insisted on a return of Crimea to Ukraine, and supported EU accession for Ukraine.[129] Estonia also embraces multilateralism and strong alliances; given the Baltic nation's technological advancement, which invites some vulnerabilities, its support of international organizations and diplomatic partnerships is understandable.

Estonian fears of Russia are well-founded. The 2007 row over Tallinn's decision to move a Soviet-era statue was a flashpoint between the two countries that has led to an array of Russian attacks. Russia's "Compatriot Policy," which was used to legitimize invasions into Abkhazia, South Ossetia, and Ukraine, still casts a shadow over Estonia given its sizeable ethnic Russian population. In addition, NATO's Strategic Communications Center (STRATCOM) reported in 2018 that Russian-language "bots" were responsible for "55 percent of all Russian-language messages about NATO in Baltic States" and that Estonia was the most frequent target of Russian bots.[130] Naturally, then, Baltic exposure to Russian hybrid warfare (an amalgamation of political, cyber, and conventional warfare) has led countries like Estonia to search for an array of countermeasures.

Estonia's Defense League (EDL, or *Kaitseliit)* is a key player in the country's countermeasure efforts. This voluntary security force, which operates under the Ministry of Defense's umbrella, has a wide range of responsibilities including physical defense, cyber defense, and even educating the public about national defense.[131] Outside of these efforts, the EDL is more directly involved with cyber defense. In 2020, it joined public and private organizations from across Europe to participate in a

128. "Mission," The Beacon Project, https://www.iribeaconproject.org/who-we-are/mission.

129. Government Communication Unit, "Ratas: Estonia is a firm supporter of Ukraine's future," Republic of Estonia Government, November 26, 2019, https://www.valitsus.ee/en/news/ratas-estonia-firm-supporter-ukraines-future; Government Communication Unit, "Ratas: The EU supports the wish of the Belarusian people to choose their own future and does not recognise the results of the presidential election," Republic of Estonia Government, August 19, 2020, https://www.valitsus.ee/en/news/ratas-eu-supports-wish-belarusian-people-choose-their-own-future-and-does-not-recognise-results.

130. NATO Strategic Communications Centre of Excellence, "Robotrolling," *Robotrolling,* no.1 (2018), https://www.stratcomcoe.org/robotrolling-20181.

131. Stephen J. Flanagan, Jan Osburg, Anika Binnendijk, Marta Kepe, and Andrew Radin, Deterring Russian Aggression in the Baltic States Through Resilience and Resistance (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2779.html.

cyberattack simulation.[132] EDL activity reflects Estonia's prioritization of joint solutions to cyber threats. The Defense League also plays a vital role in the country's fight against disinformation. It runs an anti-propaganda blog, Propastop.org, whose focus is not only on countering harmful narratives, but also on highlighting corporate practices related to social media, outing individuals and posts designed to further disinformation (e.g., "naming and shaming"), and advocating media literacy.[133]

Estonia's response to disinformation is shaped by the country's heavy reliance on digitization along with its sizable Russian population. The response is fortified by a mix of government-sanctioned measures and volunteer efforts. For example, the country created its own Russian-language channel back in 2015 as a way to counter messaging orchestrated by the Kremlin.[134] This government channel allows the broadcast of programming that is more neutral though still of interest to the Russian minority in Estonia. At the same time, the country's military leadership refuses to participate in interviews with Russian outlets to avoid having their statements misconstrued or manipulated. The country's official foreign news service, *Välisluureamet*, produces an annual report that chronicles the threats facing Estonia and is largely focused on unearthing Russian subversive measures. These efforts are laudable but often do little to counter the torrent of disinformation shared via social media.

To remedy this shortcoming, Estonian and other Baltic countries rely on citizen mobilization to counter Russian disinformation. Volunteers are supporting the EDL's response to disinformation: the so-called "Baltic Elves," an internet activist group, are involved through their work to counter Russian "trolls."[135] The "Baltic Elves" report bots, monitor news article message boards, and counter-narratives across the Baltic states. These virtual volunteers are estimated to number in the thousands and even assist Debunk.eu, which coordinates with the "elves" and Western foreign services to analyze over 20,000 articles a day to identify and counter disinformation activity.[136]

Estonia, like other Baltic countries, fears Russian threats more directly than other countries given its past Soviet occupation, the proximity to Moscow, its digital inclination, and its large Russian minority. Consequently, the country has a multifaceted approach to respond to these threats but also relies heavily on multilateralism to fend off Russian belligerence. The Baltic Cyber Defense group along with NATO's Cooperative Cyber Defense Commission and the European Union's European Extreme Action Service are much needed allies in this fight.

Multilateral Responses

Russian foreign policy has long aimed to undermine NATO and the European Union; the weaponization of disinformation has simply given the Kremlin a new way to pursue old aims. Recently, Russia has

132. ERR News, "Cyber exercise brings together Defense League, public and private sector," ERR.ee, March 6, 2020, https://news.err.ee/1060615/cyber-exercise-brings-together-defense-league-public-and-private-sector.

133. "What is Propastop?" Propastop, March 6, 2017, https://www.propastop.org/eng/2017/03/06/what-is-propastop/.

134. Aliya Sternstein, "Estonia's lessons for fighting Russian disinformation," *Christian Science Monitor*, March 24, 2017, https://www.csmonitor.com/World/Passcode/2017/0324/Estonia-s-lessons-for-fighting-Russian-disinformation.

135. Matthew Thomas, "Defeating Disinformation Threats," Foreign Policy Research Institute, February 19, 2020, https://www.fpri.org/article/2020/02/defeating-disinformation-threats/.

136. Kim Sengupta, "Meet the Elves, Lithuania's digital citizen army confronting Russian trolls," *Independent*, July 17, 2019, https://www.independent.co.uk/news/world/europe/lithuania-elves-russia-election-tampering-online-cyber-crime-hackers-kremlin-a9008931.html.

been linked to disinformation operations tying the Covid-19 pandemic with EU and NATO actions.[137] Furthermore, the Kremlin's tactics are gaining in sophistication, marrying established practices (dissemination through IRA, RT, and Sputnik and using bots to proliferate narratives) with aggressive hacking whereby false or misleading stories are posted through legitimate and credible accounts.[138]

Recognizing this threat, in 2018 the European Council endorsed a plan to counter Russian cyber threats, which included the creation of the Rapid Alert System.[139] It serves as a clearinghouse of sorts for member states to share information and concerns regarding suspected disinformation campaigns and to discuss "best practices" in responding to these malicious campaigns. The RAS then shares authoritative accounts in response to false or misleading messaging that can be disseminated by the EU member states, civil society groups, and social media companies. This mechanism has been used against Covid-19 disinformation campaigns that have spread harmful information regarding the pandemic and dangerous or unproven remedies to the disease.[140] As a multilateral, multilevel organization, the RAS has great potential to help counter Russian disinformation campaigns but it has been hampered by inconsistent participation by members, uneven real-time responses to threats, and concerns over ideologically motivated responses.[141]

NATO has also been targeted by Russian disinformation, as the Kremlin looks to sow discord and fuel animus toward the organization amid the Covid-19 pandemic.[142] False stories were spread regarding NATO's intent to withdraw troops from Lithuania, Canadian troops allegedly exposing Latvia to the virus, and a Polish military official reportedly criticizing U.S. military forces. These stories aim to undermine NATO's legitimacy and support as well as weaken individual member states.

Back in 2008, Estonia led a NATO effort to create the Cooperative Cyber Defense Center of Excellence (CCDCOE) following Russia's 2007 massive cyberattack on the Baltic nation. The CCDCOE consists of 28 member states, including the Czech Republic and Estonia, and supports a comprehensive strategy to counter cyber threats. The CCDCOE supports its mission through interdisciplinary methods to study, train, and organize exercises to fortify cyber defense. Its Locked Shields exercise is one such example of how it promotes cyber defense across teams to ensure that experts and decisionmakers are working together on these threats.[143] These efforts extend beyond disinformation alone but can contribute to ongoing efforts to curtail this influence.

---

137. Mark Scott, "Russia and China push 'fake news' aimed at weakening Europe," Politico, April 1, 2020, https://www.politico.eu/article/russia-china-disinformation-coronavirus-covid19-facebook-google/.

138. Dan Sabbagh, "Russia-aligned hackers running anti-Nato fake news campaign – report," *The Guardian*, July 20, 2020, https://www.theguardian.com/technology/2020/jul/30/russia-aligned-hackers-running-anti-nato-fake-news-campaign-report-poland-lithuania.

139. "Rapid Alert System," European Union EXTERNAL ACTION, March 15, 2019, https://eeas.europa.eu/headquarters/headquarters-homepage_en/59644/Factsheet:%20Rapid%20Alert%20System.

140. Samuel Stolton, "EU Rapid Alert System used amid coronavirus disinformation campaign," EURACTIV, March 4, 2020, https://www.euractiv.com/section/digital/news/eu-alert-triggered-after-coronavirus-disinformation-campaign/.

141. Matt Apuzzo, "Europe Built a System to Fight Russian Meddling. It's Struggling." *New York Times*, July 6, 2019, https://www.nytimes.com/2019/07/06/world/europe/europe-russian-disinformation-propaganda-elections.html.

142. "NATO's approach to countering disinformation: a focus on COVID-19," NATO, July 17, 2020, https://www.nato.int/cps/en/natohq/177273.htm.

143. "Locked Shields," CCDCOE, https://ccdcoe.org/exercises/locked-shields/.

NATO has employed other efforts to counter disinformation. In addition to CCDCOE's work, STRATCOM aims to raise awareness of information operations and refute misleading or false claims. Its analytical reports summarize tactics, messaging, and targets of Russian disinformation.[144] The organization mobilized in earnest in the wake of the Crimean annexation and since 2014 has expanded its efforts to help NATO members identify false or misleading narratives, recognize networked or coordinated Russian media activity, and increase audience resilience when targeted by the Kremlin.[145] STRATCOM's coordinated efforts are vitally important to enhance the collective security of its member states and to counter disinformation efforts levied against NATO as a whole.

Conclusion

This article underscores a few effective methods to counter disinformation operations at both the national and international levels. Estonia's use of real-time volunteer forces along with the Czech Republic's BIS and think tanks are useful in naming and shaming Russia's digital active measures. Meanwhile, Estonia's use of government-sanctioned programming can help shape the broadcast conversation, thus countering channels like RT, which further harmful narratives.

The NATO and EU responses to Russia's ongoing efforts to sow discord offer some useful suggestions for moving forward. These organizations have created task forces and organizations that, collectively, reveal a holistic framework that can help uncover subversive efforts, coordinate a cogent response, and promote multilateral collaboration. With additional buy-in from EU and NATO members, these efforts will evolve and strengthen the response to disinformation operations.

Joseph Robbins *(PhD, Texas Tech University) is the political science department head at Valdosta State University. His research examines Post-Communist party system development and, more recently, the consequences of terrorist attacks; his research has been published in journals such as* Armed Forces & Society; Comparative Politics; Comparative Political Studies; Conflict, Security, and Development; Electoral Studies; Global Policy; the Journal of East European and Asian Studies; the Journal of Peace Research; Legislative Studies Quarterly; Party Politics; and Terrorism & Political Violence.

144. The NATO Strategic Communications Center for Excellence, *Russia's Footprint in the Nordic-Baltic Information Environment* (Latvia: Nato Stratcom Center Of Excellence, 2018), https://www.stratcomcoe.org/russias-footprint-nordic-baltic-information-environment-0.

145. "Countering propaganda: NATO spearheads use of behavioural change science," Nato Stratcom Center Of Excellence, May 12, 2015, https://stratcomcoe.org/countering-propaganda-nato-spearheads-use-behavioural-change-science.