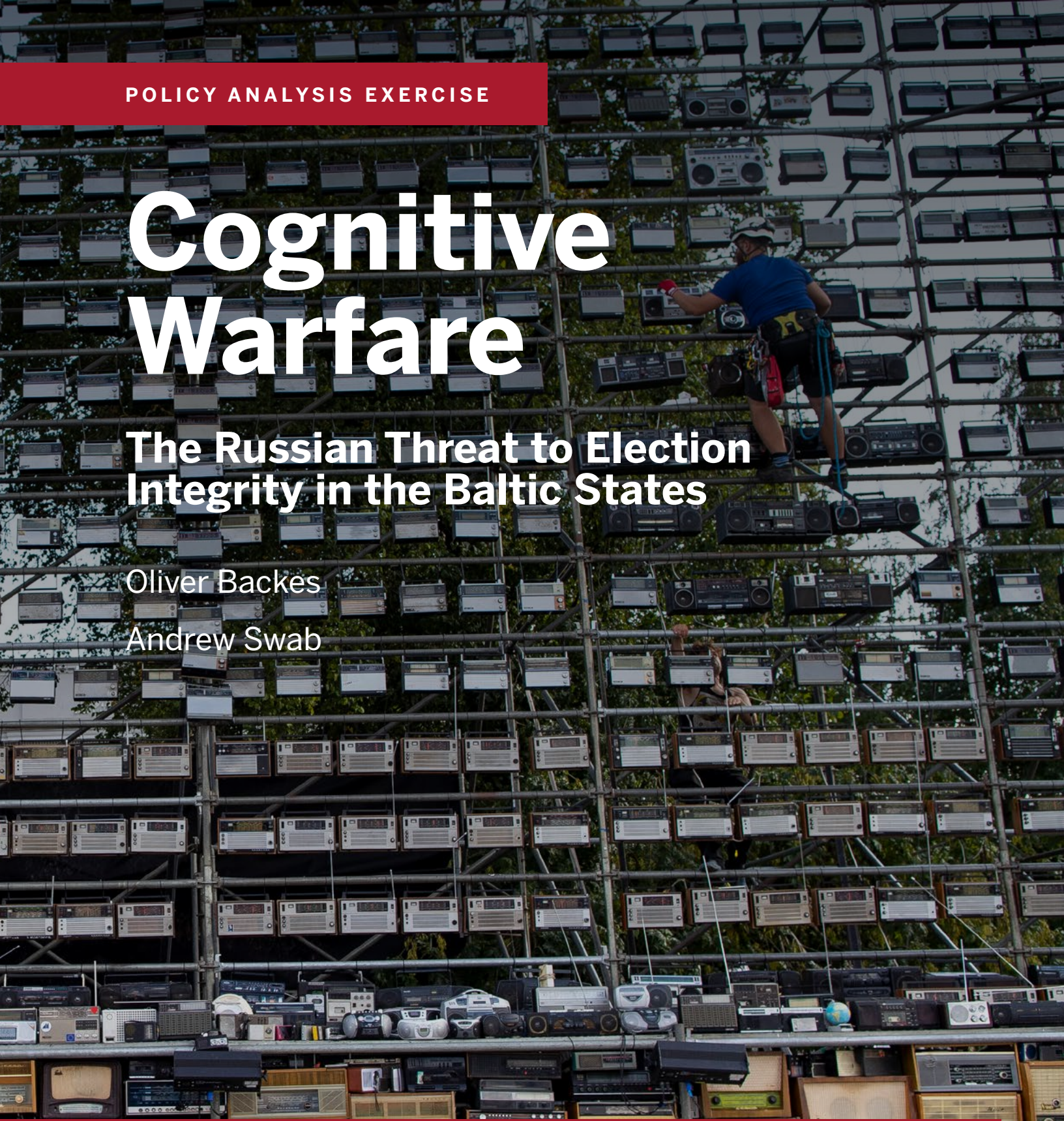
POLICY ANALYSIS EXERCISE

Cognitive Warfare

The Russian Threat to Election Integrity in the Baltic States

Oliver Backes

Andrew Swab



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
NOVEMBER 2019

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org

This paper was completed as a Harvard Kennedy School Policy Analysis Exercise, a yearlong project for second-year Master in Public Policy candidates to work with real-world clients in crafting and presenting timely policy recommendations.

Cover photo: A technician prepares a giant construction made up of nearly 1,500 old radios on Vilnius Cathedral square, to commemorate events of 1989 when analog radios were used to coordinate the so-called Baltic Way human chain, in Vilnius, Lithuania, Friday, Aug. 23, 2019. (AP Photo/Mindaugas Kulbis)

About the Authors

Oliver Backes graduated with a Master in Public Policy degree from the Harvard Kennedy School of Government in May 2019, concentrating in international and global affairs. Before HKS, he spent five years working with the Russia and Eurasia Program (REP) at the Center for Strategic and International Studies (CSIS) in Washington, D.C. At CSIS, his research and analytical work focused primarily on Russian foreign and domestic policy, including the conflict in Ukraine, and the economic and geopolitical dynamics of Eurasia, with a particular emphasis on the states of Central Asia and the South Caucasus. He worked this summer as a research assistant with the Future of Diplomacy Project at the Belfer Center for Science and International Affairs at HKS focusing on NATO issues. Oliver holds a B.A. in international relations and history from the University of Pennsylvania.

Andrew Swab graduated with a Master in Public Policy degree from the Harvard Kennedy School of Government in May 2019. Last summer, he was a Kenneth I. Juster Fellow in the U.S. Department of the Treasury, where he supported efforts to understand emerging financial technologies, and improve cybersecurity in the U.S. financial sector. At HKS, he was a teaching assistant for Professors Graham Allison and David Sanger. Before HKS, Andrew worked at the U.S. Department of State as a security policy analyst with a portfolio that covered diplomatic missions in Europe and Eurasia. Before this, he worked for the foreign affairs desk at the PBS NewsHour. Andrew holds a B.A. in international relations and journalism from Syracuse University. His family is Latvian-American, adding a personal connection to this project. His dedicates his portion of the project to his great-grandmother Elsa Schulmeister, who came to the United States from Latvia for the ideas of freedom, opportunity, and democracy.

Table of Contents

Acknowledgments

We would like to express our gratitude to our advisors, Professor Stephen M. Walt and Professor Dara Kay Cohen, for their guidance and feedback on this project. We would also like to thank Eric Rosenbach, who provided valuable help throughout this project, and the Belfer Center for Science and International and Affairs for the recognition of our work with the Robert Belfer Annual Award for Best Policy Analysis Exercise, and for funding our field research in Tallinn, Estonia; Riga, Latvia; and Vilnius, Lithuania in January 2019. We would like to express our appreciation for the Belfer Center's Defending Digital Democracy Project (D3P), whose prior work developing strategies, tools, and recommendations to protect democratic processes proved invaluable.

We would also like to thank our clients, the embassies of Estonia, Latvia, and Lithuania in Washington D.C., for their work with us on this project. Specifically, we would like to thank Kadri Peeters, Rolands Henins, and Vaidotas Urbelis – from the embassies of Estonia, Latvia, and Lithuania in Washington, D.C. respectively – for their invaluable guidance and support. We would also like to thank Kersti Luha, Anda Zule, and Zivile Vaicekauskaite for their support on the ground in Tallinn, Riga, and Vilnius.

About the Authors

Oliver Backes graduated with a Master in Public Policy degree from the Harvard Kennedy School of Government in May 2019, concentrating in international and global affairs. Before HKS, he spent five years working with the Russia and Eurasia Program (REP) at the Center for Strategic and International Studies (CSIS) in Washington, D.C. At CSIS, his research and analytical work focused primarily on Russian foreign and domestic policy, including the conflict in Ukraine, and the economic and geopolitical dynamics of Eurasia, with a particular emphasis on the states of Central Asia and the South Caucasus. He worked this summer as a research assistant with the Future of Diplomacy Project at the Belfer Center for Science and International Affairs at HKS focusing on NATO issues. Oliver holds a B.A. in international relations and history from the University of Pennsylvania.

Andrew Swab graduated with a Master in Public Policy degree from the Harvard Kennedy School of Government in May 2019. Last summer, he was a Kenneth I. Juster Fellow in the U.S. Department of the Treasury, where he supported efforts to understand emerging financial technologies, and improve cybersecurity in the U.S. financial sector. At HKS, he was a teaching assistant for Professors Graham Allison and David Sanger. Before HKS, Andrew worked at the U.S. Department of State as a security policy analyst with a portfolio that covered diplomatic missions in Europe and Eurasia. Before this, he worked for the foreign affairs desk at the PBS NewsHour. Andrew holds a B.A. in international relations and journalism from Syracuse University. His family is Latvian-American, adding a personal connection to this project. His dedicates his portion of the project to his great-grandmother Elsa Schulmeister, who came to the United States from Latvia for the ideas of freedom, opportunity, and democracy.

Executive Summary

Recent years have seen a cascade of revelations regarding Russian attempts to interfere with or disrupt elections in the West. While the Russian government's influence campaign in the 2016 US presidential election is the most well-known, it was by no means an isolated incident. Western governments are waking up the threat that Russian cyber and information operations pose to the integrity of their elections and the stability of their domestic politics. However, the question of how to counter these efforts remains unanswered.

The goal of this report is to offer an answer to two questions:

(1) How do we understand the Russian threat to election integrity?
(2) What can governments do to counter such efforts or mitigate their impact?

Our specific focus is on Russian election interference efforts in Estonia, Latvia, and Lithuania, which have a long history dealing with and responding to Russian political interference. By studying the mechanisms through which Russia seeks to undermine domestic political processes in the Baltic states, we can better understand the threat that Russia poses. And by analyzing the policies that the Baltic governments have implemented over the last three decades, we can better assess the effectiveness of countermeasures and determine how Estonia, Latvia, Lithuania, and their Western allies should counter election interference in the future.

The current Western discourse emphasizes two vectors of malign Russian interference in elections. The first is the cyber vector, through which Russia uses cyber capabilities to compromise sensitive election systems (and other government networks) with the goal of affecting the election outcome. The second is the information vector, through which Russia injects disinformation, propaganda, and leaked or stolen documents into the domestic political discourse in order to inflame divisions within a society, undermine its politics and institutions, and affect the election outcome.

Russian strategy emphasizes the information vector over the cyber vector. Russia primarily interferes in the democratic processes of the Baltic states using information means, with cyber playing a secondary, enabling role. The Kremlin considers disinformation and information operations to be the most effective means of affecting political outcomes in other countries. Russia seizes on existing domestic political, social, or ethnic divisions and instrumentalizes them to change how voters think – and through that how they vote.

We have termed this strategy "cognitive warfare" – altering through information means how a target population thinks, and through that, how they act. Russia has employed a cognitive warfare strategy in the Baltic states for years. Russian has pushed, through traditional and social media, narratives designed to divide ethnic Russians and Russian-speakers from the rest of the society, undermine domestic political stability, and break the Baltic commitment to the EU and NATO. Russia's cognitive warfare efforts have not always met with success or

improved the electoral results of pro-Russian political forces; however, the strategy has been consistent since the Baltic states regained their independence in the early 1990s.

At present, the threat that cognitive warfare operations pose to election integrity is greater than the threat posed by Russian cyber capabilities. We assess a low level of risk to the scenario in which Russia successfully, undetectably compromises election systems and alters an election outcome in the Baltic states. That is not to say the governments of the Baltic states do not – or should not – emphasize cybersecurity countermeasures. On the contrary, all three Baltic governments have rightly developed robust cybersecurity protections for their election systems and implemented monitoring or post-election auditing procedures to protect against foreign compromise.

In our view, the most significant cyber risk to election integrity derives from inadequate cybersecurity protections put into place by other politically-relevant actors, particularly political campaigns, political parties, and media. Russian hackers regularly target these organizations, stealing sensitive, private information that the Kremlin later integrates into interference and influence campaigns in the Baltic states. Rather than posing a direct threat to election systems, Russian cyber actors more often work to enable later information operations.

What should governments do? We assess that the approaches taken by the Estonian, Latvian, and Lithuanian governments to counteract and mitigate the impact of Russian interference efforts are sound and should continue. Responding to a cognitive warfare strategy is not merely a technical problem – it is a society-wide information challenge, requiring more than simply debunking fake news or removing fake accounts on Facebook or Twitter. We recommend that these governments build upon their efforts in several areas:

- Expand investments in election cybersecurity;
- Provide additional resources to working groups on election security and disinformation;
- Exercise and stress-test election-related contingency plans;
- Deepen sharing of intelligence, best practices, and lessons learned with allies;
- Invest in the monitoring of disinformation and explore regulatory approaches;
- Expand integration policies targeting Russian minority populations; and
- Craft and promote compelling, unifying national narratives.

We believe that adopting this set of recommendations will enhance the effectiveness of the Baltic governments in responding to Russian interference in the short-term and promote greater societal resilience to cognitive warfare campaigns over the long-term.

Other Western governments can learn from the experience of the Baltic states as well. If the experiences of Estonia, Latvia, and Lithuania are a guide – and we believe that they are – it is Russia's cognitive warfare strategy and information operations, not cyber threats, that pose the greater threat to election integrity on both sides of the Atlantic. The Kremlin's goal is to undermine Western elections by interfering with the minds of voters, not our digital voting systems. Simply improving the security of those systems will not be sufficient to meet this threat.

Russia weaponizes our domestic political, social, and cultural divisions, turning them against us and using them to undermine the integrity of our electoral processes.

Western governments should also be clear-eyed in recognizing that mitigating the impact of Russian political interference campaigns is a long-term problem. This is the work of decades, not years. Russian interference is not a problem that can be easily solved; instead, Western governments will have to manage it for years to come. Just as cognitive warfare relies on our domestic vulnerabilities to function, so too will the Russian threat to election integrity not be fully mitigated as long as those vulnerabilities persist.

Methodology

Given that Russian cyber and information operations evolve and adapt to new technologies and political conditions, academic and think tank research on these topics becomes quickly dated for its application to present-day public policy problems. We developed a research methodology that relied on the most up-to-date research and scholarship. The components of our methodology were as follows:

- A comprehensive review of the current literature on Russian cyber and information operations and the threat to elections;
- Open-source research on these same topics, with a focus on news and reporting;
- Elite interviews – 45 in total – with government officials, academics, and experts on foreign policy, elections, and related topics in Estonia, Latvia, Lithuania, and the US;[1]
- Fieldwork in Tallinn, Estonia; Riga, Latvia; and Vilnius, Lithuania in January 2019.

Our findings and analysis draw heavily on our elite interviews – and in particular on our conversations in Tallinn, Riga, and Vilnius. During our fieldwork in the Baltic states, we used a semi-structured interview format based on a templated list of research questions. We tailored our interview questions to the specific expertise or policy focus of our interviewees to ensure that we were capturing the most accurate, relevant information on which to base our analysis.

A full list of the organizations and ministries with which we met, and a list of our research questions can be found in Appendices 1 and 2, respectively.

This report used human-subject protection protocols and standards set by the Institutional Review Board (IRB) at Harvard Kennedy School. These standards also comply with those put forward by Harvard University's Committee on the Use of Human Subjects in Research (CUHS), located in Harvard's Office of the Provost for Research.

Limitations and Biases

This study is limited in part by our slate of interviewees. We primarily interviewed government officials, academics, and other policy professionals. Our interviews included meetings with civil society organizations, inter-governmental organizations, and think tanks. However, we conducted the bulk of our interviews with government officials in Estonia, Latvia, and Lithuania. We operated under the assumption that our interviewees were honest and candid with us and have no reason at this time to doubt the validity of that assumption. Where possible, we cross-checked our interviews with publicly-available information.

[1] For purposes of satisfying interview confidentiality and reporting accurately, we will refer to elite interview sources in this report as "an Estonian/Latvian/Lithuanian X official," where X refers to the area of expertise or ministry. When appropriate, we named sources, but only if the source had given consent to have their quote and name published. We believe this process lends credibility to our research as it increased the level of candor about an issue that has political, economic, and intelligence concerns.

We acknowledge interviewees may have their own biases. Still, we believe capturing *viewpoints* matters for this kind of research, especially when the focus of the research is to understand the risk perception within the Baltic states and how these governments understand the Russian threat. Additionally, comprehensive, high-quality quantitative data on the impact of Russian information operations, propaganda, and disinformation is in short supply. As such, this report relies heavily on qualitative data. It is supplemented by quantitative data where possible, with a particular focus on demography and public opinion. This study is also limited in understanding how information operations directly affect individual citizens. We were not able to conduct interviews or focus groups with regular citizens.

A further limitation regards the specifics of cybersecurity protections in the Baltic states. We were not able to discuss or assess the detailed technical specifics of the cybersecurity protections defending Baltic election systems. This information is generally not shared publicly. We based the assessment of cybersecurity vulnerabilities on discussions with elections and cybersecurity officials, outside experts, and a literature review.

An additional issue stems from potential pro-EU, and pro-NATO bias of our interviewees, and clients. Generally, the governments of the Baltic states favor integration into NATO and the EU. At the same time, the Baltic states have a long, fraught history with Russia. Government officials often stated viewpoints that reflected this history. The individuals we interviewed were, to a person, committed to the Baltics remaining free, prosperous European states inside NATO and the EU. Much of this report focuses on Russia's efforts to break that commitment and undermine the sovereignty of these states. We acknowledge our bias on this issue – our goal is solely to provide research and analysis that improves outcomes for our clients and furthers their goals. As such, in this report, we treat Russian efforts not as one side in an even-handed discourse, but as a threat to be countered.

Conceptualizing the Russian Threat to Election Integrity

- Elections are a time of unique vulnerability in democratic societies that Russia exploits.
- Protecting election integrity is a society-wide information challenge.
- The current Western discourse overemphasizes the cyber threat to election systems. The Kremlin views cognitive warfare strategies as the most effective.
- Western governments should reweight their risk portfolios and place greater emphasis on the information threat to election integrity.

Election periods are a time of unique vulnerability in democratic societies. They are moments of round-the-clock campaigning, non-stop media coverage, breathless public debate, and high domestic political and social tension. Elections surface the issues and identities that divide our societies. Most importantly, elections are the sacred moment in time when voters express their will, passing judgment on their governments and determining the future of their countries.

Russia seeks to take advantage of these moments of unique vulnerability. Russia interferes in the elections of the Baltic states and other Western governments to advance its geopolitical interests, undermine the politics and institutions of its adversaries, and divide the transatlantic alliance. It does so primarily through both information and cyber means – a toxic strategic combination that we are calling "cognitive warfare." During elections, the public requires information to make an informed decision at the ballot box. **Russia tries to manipulate the information voters receive, injecting disinformation and propaganda into the media ecosystem in order to, in the words of Vladislav Surkov – a close adviser to Russian President Vladimir Putin – "interfere in your brains and change your conscience."**[2] Russia's misuse of the information ecosystem and use of cyber capabilities poses a severe and unique threat to Western political systems – undermining public trust in the electoral process, compromising voting systems, and, in theory, affecting the election outcome.[3]

Recent years have seen a cascade of revelations regarding Russian efforts to affect or disrupt electoral processes in Western states. The Russian government's influence campaign in the 2016 US presidential election is not an isolated incident. Russia reportedly interfered in the 2016 Brexit referendum in the United Kingdom,[4] the campaign of Emmanuel Macron in the 2017

[2] Vladislav Surkov, "Долгое государство Путина," *Независимая газета*, February 11, 2019, http://www.ng.ru/ideas/2019-02-11/5_7503_surkov.html.
[3] Office of the Director of National Intelligence, "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections," January 6, 2017, ii, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[4] Francesca Gillett, "Electoral Commission launches probe into Russian meddling in Brexit vote using Twitter and Facebook," *The Evening Standard*, November 2, 2017, https://www.standard.co.uk/news/politics/election-watchdog-launches-probe-into-russian-meddling-in-brexit-vote-a3674251.html.

presidential election in France,[5] the 2017 general elections in the Netherlands,[6] the 2019 EU elections in Italy,[7] and is reportedly planning to interfere again in the US in 2020.[8] Governments on both sides of the Atlantic rightly see themselves as potential future targets

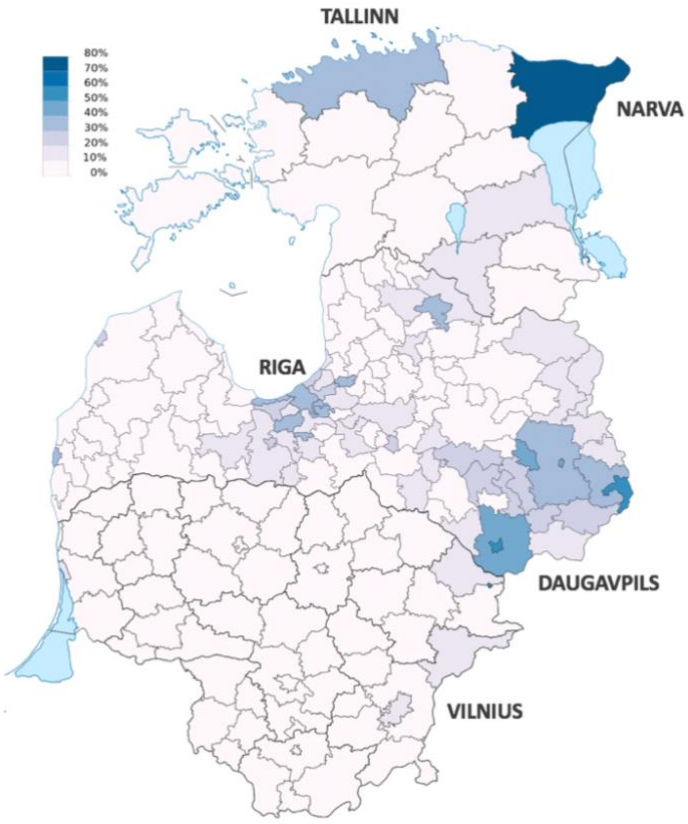
Russia's aggressive campaign of political interference has made protecting the integrity of elections a top priority for Western governments. Yet, despite significant policy attention, the question of how to most effectively counter Russian efforts or mitigate their impact on domestic political processes is a question that – as of this writing – remains unanswered. Answering these questions is the goal of this report:

How do we understand the Russian threat to election integrity? And how can governments most effectively counter or mitigate their impact on domestic political processes?

Understanding the Baltic States

To understand the nature of the Russian threat, we must first understand the demographics and historical experience of the three Baltic states – Estonia, Latvia, and Lithuania. All three Baltic countries have substantial populations that are either ethnically Russian or speak Russian as their primary language. As **Figure 1** shows, ethnic Russians and Russian-speakers are concentrated in the city of Narva, on the Estonian border with Russia, in the Tallinn and Riga metropolitan areas, and near Daugavpils in the Latgale region of southeast Latvia. Smaller communities inhabit the coastal portion of Lithuania near the border with Kaliningrad and around Vilnius.

Figure 1: Ethnic Russians in the Baltic States at the Local Level, by Percentage of Total Population, 2011



Source: Wikimedia Commons, Creative Commons Attribution Share Alike 3.0

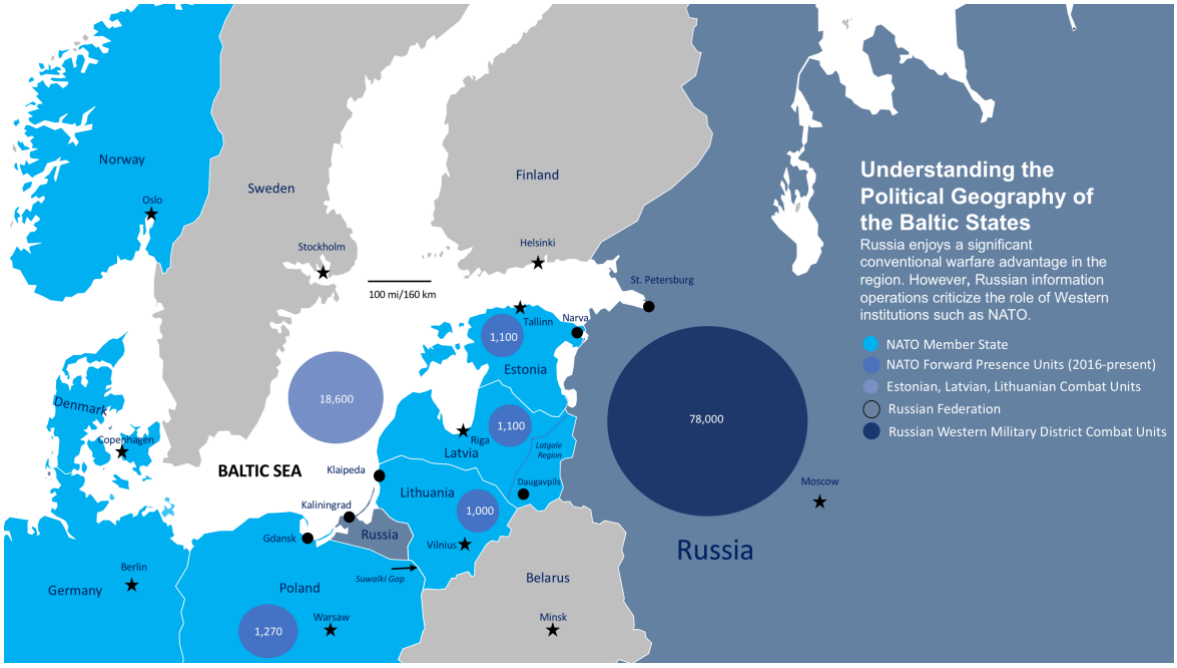
[5] Jean-Baptiste Jeangene Vilmer, *Successfully Countering Russian Electoral Interference: 15 Lessons Learned from the Macron Leaks* (Washington: Center for Strategic and International Studies, June 2018), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180621_Vilmer_Countering_russiam_electoral_influence.pdf?qFOz5qjpEuTzu5cvUa.UgOj0Dg3FklQP.

[6] Cynthia Kroet, "Russia spread fake news during Dutch election: report," *Politico*, April 4, 2017, https://www.politico.eu/article/russia-spread-fake-news-during-dutch-election-report-putin/.

[7] Andrew Rettman, "Exposed: How Russia offered to fund Italy's Salvini," *EuroOberver*, February 25, 2019, https://euobserver.com/foreign/144253.

[8] Uri Friedman, "Here's What Foreign Interference Will Look Like in 2020," *The Atlantic*, August 9, 2019, https://www.theatlantic.com/politics/archive/2019/08/foreign-election-interference-united-states/595741/

Figure 2: The Political Geography of the Baltic Region



The Baltic states are in a unique position vis-à-vis Russia among NATO and EU members. The Soviet Union occupied all three states during World War II and the Cold War, and all three transitioned to well-functioning electoral democracies post-independence, subsequently entering the EU and NATO. Estonia and Latvia share a land border with Russia, while Lithuania shares a border with Kaliningrad, a Russian enclave. Each state has been the target of a persistent campaign of Russian political interference since regaining their independence in the early 1990s.[9]

As **Figure 2** illustrates, Russia has a significant conventional military force in the region – 78,000 combat units stationed in its Western Military District.[10] NATO counterbalances this force with forward-deployed NATO units in the Baltic states and Poland to supplement Estonian, Latvian, and Lithuanian combat units. While Russia uses non-military means, such as information and cyber operations to try to undermine the Baltic states and divide them from NATO and the EU, it retains a conventional military advantage in the region.

During their occupation, the Soviets subjected the Baltic states to policies of "Russification."[11] Thus, the ethnic Russian populations in Estonia constitutes about 24.9 percent of the total and 25

[9] A number of our interviewees throughout the Baltics emphasized that Russian political interference and disinformation efforts extend back well beyond the 1990s to the occupation of Estonia, Latvia, and Lithuania during the Soviet period. One official noted that observers should see Russia's current policies as a continuation of both Soviet and Tsarist policy extending back more than a century.

[10] Scott Boston, Michael Johnson, Nathan Beauchamp-Mustafaga, and Yvonne K. Crane, Assessing the Conventional Force Imbalance in Europe: Implications for Countering Russian Local Superiority (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR2402.html.

[11] John R. Beyrle, "The Long Good-Bye: The Withdrawal of Russian Military Forces from the Baltic States," *Institute for the Study of Diplomacy*, *Georgetown University*, 1996, p. 1.

percent of the total population in Latvia.[12] The proportion is smaller in Lithuania – around 15 percent of the total population.[13] As a result of the Soviet occupation, the populations of the Baltic states have a profoundly ambivalent relationship with Russia – deep antipathy exists alongside equally deep historical, political, economic, and cultural ties. Influence operations short of war target these populations with narratives that portray NATO and the EU negatively and enflame existing social, economic, political, ethnic, and linguistic grievances.

An understanding of this political and military geography helps to underscore the situation of the Baltic states and the threat they face from Russia. While the US and Western Europeans have recently awakened to the nature of this threat, the Baltic governments have lived with it much longer. This history informs their perception and understanding of Russian efforts to affect their electoral processes and compromise digital systems essential to national security. The Baltic states thus provide a unique window into the full spectrum of subversive measures that form the basis for more recent Russian election interference campaigns.

Goals of this Report

The goals of this report are threefold: The first is to **present our findings** on the current state of election security, counter-disinformation, and societal resilience policy in the Baltic states. Our goal is to outline what Estonia, Latvia, and Lithuania have done to mitigate the effects of Russian efforts, to explain how these governments have experienced the Russian threat, and to determine how Russia has sought to advance its interests in these countries.

The second goal is to **provide actionable recommendations** to the governments of Estonia, Latvia, and Lithuania for safeguarding election integrity and enhance societal resilience to foreign interference. While the policy approaches that governments have implemented to date are useful and should be maintained, the Baltic states face the problem of building resilience to mitigate and manage constant Russian interference. The report provides suggestions, tailored to the specific context of each of Estonia, Latvia, and Lithuania, which could be integrated into each government's existing approach and enhance their overall effectiveness.

The third goal is to **draw out lessons and policy innovations** from the Baltic states that are relevant to the concerns of other Western democracies. Estonia, Latvia, and Lithuania have been developing policies to counteract Russian political subversion and disinformation efforts for much longer than most of their Western allies. The experiences of Estonia, Latvia, and Lithuania can and should act as a guide to other Western governments on election security. While the Baltic experience is not perfectly analogous, we believe that when the US and other European partners develop national strategies for ensuring election integrity, they should first take an in-depth look at how the Baltic states counteracted similar efforts in the past.

[12] Statistics Estonia, "Population by Sex, Ethnic Nationality and County," January 1, 2018, accessed March 31, 2019, https://www.stat.ee/population-indicators-and-composition and Latvian Central Statistical Database, 2018, accessed March 31, 2019, https://data.csb.gov.lv/pxweb/lv/iedz/iedz__iedzrakst/IRG080.px/?rxid=cd00d9dc-a4e4-4b85-a975-e8b416dee23e.

[13] Agnia Grigas, "Compatriot Games: Russian-Speaking Minorities in the Baltic States," *World Politics Review*, October 21, 2014, https://www.worldpoliticsreview.com/articles/14240/compatriot-games-russian-speaking-minorities-in-the-baltic-states.

The Current Western Discourse

Many Western governments only recently recognized the threat that Russian political interference and disinformation campaigns pose to their domestic political processes and institutions. Several government officials in our interviews in Estonia, Latvia, and Lithuania emphasized that recognition within the EU and NATO of the threat that Russian cyber and disinformation campaigns pose to member states has increased dramatically in the last few years. Russia's 2014 annexation of Crimea and the 2016 interference in the US election were, in their estimation, clear inflection points.[14] Even so, there is not yet unanimous agreement about how to best counter Russian efforts.

The last half-decade has been a period of debate, analysis, and introspection within Western democracies. Governments continue to assess their vulnerability to Russian election interference and have developed an array of policy responses. Evaluations of the election security risk portfolio within Western states broadly coalesced around two sets of threat vectors: 1) cyber compromise of election-related systems and 2) coordinated disinformation and information operations.[15]

In the current discourse, officials and analysts emphasize traditional election security concerns – namely the technical cybersecurity of election systems and the threat that compromise of these systems by Russian cyber actors poses to election integrity.[16] [17] [18] Such concerns are not purely theoretical. The US intelligence community assessed with high confidence that during the 2016 presidential campaign Russian hackers "obtained and maintained access to elements of multiple US state or local electoral boards," though notably not to systems involved in the tallying of votes.[19] A US Senate report later stated Russian hackers had the ability to "at a minimum, alter or delete voter registration data" in several states.[20] Worries about the prospect of Russia using cyber means to alter vote tallies in future elections remains a live issue. It is important to note, however, that there is currently no evidence of Russia possessing the capacity to alter votes directly – or of Russia having ever done so.

[14] Interviews with Estonian, Latvian, and Lithuanian government officials, January 14-24, 2019.
[15] Other vectors for political subversion or interference in political processes, including financial and economic compromise of political actors, tend not to figure as prominently in U.S. and Western European analyses. These factors are, however, important elements of the risk portfolio facing Estonia, Latvia, Lithuania, and many other states in Eastern and Central Europe.
[16] Laura Galante and Shaun Ee, *Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents* (Washington: The Atlantic Council, September 2018), https://www.atlanticcouncil.org/images/publications/Defining_Russian_Election_Interference_web.pdf, 5.
[17] Benjamin Wafford, "The hacking threat to the midterms is huge. And technology won't protect us." *Vox*, October 25, 2018, https://www.vox.com/2018/10/25/18001684/2018-midterms-hacked-russia-election-security-voting.
[18] Eric Rosenbach, "America, Democracy and Cyber Risk: Time to Act," Testimony to the United States Senate Committee on Homeland Security and Governmental Affairs, April 24, 2018, https://www.hsgac.senate.gov/imo/media/doc/Testimony-Rosenbach-2018-04-24.pdf.
[19] "Intelligence Community Assessment," iii.
[20] Senate Intelligence Committee, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," May 8, 2018, https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

Western officials and analysts also emphasize the Russian threat in the information sphere. Russia injects disinformation, propaganda, and false narratives into the media environments of adversary states, often through social media.[21] Russia capitalizes on existing social and cultural fissures to undermine domestic political cohesion more broadly. These efforts also often appear designed to influence electoral outcomes and advance the political fortunes of Russia-friendly candidates or political parties – though this is by no means always the case.[22]

Protecting election integrity is much more than simply a technical or security problem – it is a society-wide information challenge.

The question of how to respond to or counter Russian information operations remains largely unresolved. The debate on this issue focuses on policies concerning social media and the role of platforms like Facebook and Twitter in providing a vehicle for Russian disinformation campaigns.[23] [24] Senior executives from social media platforms testified about Russian interference in political systems before legislatures on both sides of the Atlantic in past years, but Western policymakers have not *directly* addressed the disinformation challenge itself. Western publics debate the thorny questions surrounding the role of government in addressing the disinformation phenomenon on these platforms. Meanwhile, Facebook, Twitter, and others have taken small steps to address Russian activity on their platforms, including, for example, robust efforts to delete fake accounts. But these self-regulation efforts appear insufficient to address the full scope of the disinformation problem.[25]

Reweighting the Risk Portfolio

We assess that Western governments must reweight the risk portfolio to emphasize the threat from information operations to elections over direct technical interference with election systems. If the Baltic experience is a guide (and we believe that it is), **protecting election integrity is much more than merely a technical or security problem – it is a society-wide information**

[21] Eitvydas Bajarunas, "Lessons from the Baltic States: strengthening EU resilience against Russian hybrid warfare," in *Hybrid and Transnational Threats: Discussion Paper*, Jamie Shea, ed. (Brussels: Friends of Europe, 2018), https://www.friendsofeurope.org/sites/default/files/2018-12/FoE_SEC_PUB_Hybrid_DP_WEB.pdf, 25-26.
[22] See Mike Winnerstig, ed., *Tools of Destabilitization: Russian Soft Power and Non-military Influence in the Baltics States* (Stockholm: FOI, 2014), http://appc.lv/wp-content/uploads/2014/12/FOI_Non_military.pdf.
[23] Todd C. Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, Zev Winkelman, "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe," (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf, 11.
[24] Galante and Ee, 5.
[25] Dustin Volz and Joseph Menn, "Twitter suspends Russia-linked account, but U.S. senator says response inadequate," *Reuters*, September 28, 2017, https://www.reuters.com/article/us-usa-trump-russia-twitter-idUSKCN1C331G. See also Margaret Hartmann, "Facebook Haunted by Its Handling of 2016 Election Meddling," *New York Magazine*, March 20, 2018, http://nymag.com/intelligencer/2018/03/facebook-haunted-by-its-handling-of-2016-election-meddling.html.

challenge.[26] Reweighting the risk portfolio does not imply the Baltic states and their Western allies should ignore the threat that Russian cyber capabilities pose to their election systems. On the contrary, Baltic governments rightly prioritize election cybersecurity – and continued investment in the security of election infrastructure remains a necessity. However, it will be necessary for Western governments to place significantly greater emphasis on the cognitive and information aspects of Russia's strategy and address directly the multiple vectors through which Russian tactics undermine political stability and affect election outcomes.

Russian efforts to interfere in the domestic politics of Estonia, Latvia, and Lithuania suggest **the Kremlin views disinformation and influence operations as the most effective and efficient means of affecting political outcomes**. Cyber operations and efforts to compromise critical technical systems – including elections infrastructure – have played a secondary role in Russian strategy, complimenting and providing ammunition for a coordinated, persistent set of information operations in the Baltic states that have lasted decades. Russia's interference campaigns in the US in 2016 and throughout Europe feature a similar strategic emphasis. In both these cases, the core of Russian efforts to affect election outcomes consisted of the strategic release of damaging information and a coordinated campaign of disinformation on social media rather than efforts to compromise election systems and alter voting results.

While instructive, we do not see the Baltic experience as perfectly analogous to that of other Western states. As will be discussed in greater detail in the section of this report on "Lessons for Western Democracies," Estonia, Latvia, and Lithuania are in many ways in a unique position vis-à-vis Russia. Geographic proximity, historical and cultural ties, the presence of ethnic Russian and Russian-speaking populations, and the overlap of the Russian and Baltic media environments are just a few of the particularities that complicate efforts to draw universally-applicable lessons from the Baltic experience. While Western policymakers should not adopt wholesale either the Estonian, Latvian, or Lithuanian approach to these issues, they should take an in-depth look at the policy approaches adopted by these governments – and integrate relevant aspects into their national strategies.

[26] For this report, election integrity is distinct from election security. While the latter is concerned with whether votes are counted safely and securely, the former is concerned with whether the votes cast reflect the interests of a foreign power.

The Cognitive Warfare Threat to Election Integrity

- Cognitive warfare – Russia's strategy that focuses on altering through information means how a target population thinks – is the primary threat to election integrity in the Baltics.
- Russia uses information operations to enflame domestic divisions within the Baltic states, undermine their domestic politics and institutions, and affect election outcomes.
- Russia deploys a consistent set of narratives in their propaganda and disinformation: instrumentalization of historical memory, claims that the Baltics are failing states, and appeals to Russian ethnic and linguistic minorities.
- Mitigating the impact of Russian political interference is a long-term challenge, requiring policy interventions to build up societal resilience.

Russia's Cognitive Warfare Strategy

Russia attempts to undermine election integrity in the Baltic states through a persistent strategy of cognitive warfare. **Cognitive warfare is a strategy that focuses on altering how a target population thinks – and through that how it acts**. For this report, we separate this term from the current discourse on Russian "hybrid warfare" strategies and tactics. The power of the cognitive warfare framing is that it allows us to examine Russia's strategy separately from the other dimensions of military power. Cognitive warfare is specific to the domestic information environments of the Baltic states (and other Western countries) and takes as its overarching goal to undermine or shape domestic political processes by changing mindsets. Cognitive warfare weaponizes information to persuade or confuse populations and shift public opinion, often tapping into real divisions in Baltic societies to drive wedges between the state and potentially sympathetic populations.

Figure 3 situates cognitive warfare and the threat it poses to election integrity within the overall structure of Russian foreign policy and grand strategy. This figure borrows from the concept of the operational levels of war. At the level of foreign policy and grand strategy, Russia aims to restore its great power status, maintain influence in what it perceives to be its "near-abroad," and desires to exacerbate

Figure 3: Conceptualizing Cognitive Warfare in the Baltic States

Source: Adapted from Scott Boston and Dara Massicot, *The Russian Way of Warfare: A Primer* (Santa Monica, CA: RAND Corporation, 2017), https://www.rand.org/pubs/perspectives/PE231.html.

divisions in the EU and NATO. Cognitive warfare operates at the strategic level, intending to undermine and divide target societies during peacetime through non-kinetic means. At the operational level, the cognitive warfare strategy relies upon information operations, or the collection and dissemination of disinformation, propaganda, and politically-sensitive information (both fake and genuine) in the Baltic states. At the tactical level, this includes the use of propaganda and related political subversion efforts, distributed through both traditional and social media.

We are not the first to use the term "cognitive warfare." It has appeared – if only sporadically – in the national security literature in recent years.[27] We, however, see the definition of Russia's cognitive warfare strategy that we have put forward as distinct. Our focus is on Russia's strategy to achieve political ends through non-kinetic actions that **alter how a population thinks during peacetime**. Additional literature on the topic has emphasized cognitive warfare as non-kinetic in nature but in a military context, and speaks to how state and non-state organizations can use it on the internet and on social networking platforms.[28] Put simply, if war is the continuation of politics by other means, then cognitive warfare is the manipulation of the politics of foreign countries through new media.

The battlespace for cognitive warfare is the mindset of the population – the six inches between the ears of every Estonian, Latvian, and Lithuanian citizen.

Russia's objective in the Baltic states is to undermine institutions, advance pro-Russian political forces, and create domestic instability, all with the long-term goal of advancing Russian interests in the region and dividing the Baltics from their Western partners. Cognitive warfare is central to this overall strategy. The battlespace for cognitive warfare is the mindset of the population – the six inches between the ears of every Estonian, Latvian, and Lithuanian citizen**.** As Vladislav Surkov, a close advisor to Russian President Vladimir Putin writes, Russia's goal is to "interfere in your brains [and] change your conscience."[29] Through persuasion, appeals to ethnic identity and historical memory, and the dissemination of false information that enflames domestic

[27] Kimberly Underwood, "Cognitive Warfare Will Be Deciding Factor in Battle," *SIGNAL Magazine*, August 15, 2017, https://www.afcea.org/content/cognitive-warfare-will-be-deciding-factor-battle and Emily Bienvenue, Zac Rogers, Sian Troath, "Cognitive Warfare: The Fight We've Got," *Cove*, September 19, 2018, https://www.cove.org.au/adaptation/article-cognitive-warfare-the-fight-weve-got/.
[28] Gabi Siboni, "The First Cognitive War," in *Strategic Survey for Israel 2016-2017*, eds. Anat Kurz and Shlomo Brom (Tel Aviv: Institute for National Security Studies, 2016), https://www.inss.org.il/publication/first-cognitive-war/.
[29] Surkov, "Долгое государство Путина."; Cristina Maza, "Vladimir Putin's Adviser Tells Americans: 'Russia Interferes in Your Brains, We Change Your Conscience'," *Newsweek*, February 12, 2019, https://www.newsweek.com/russia-president-vladimir-putin-election-americans-1327793.

grievances, Russia attempts to alter how the populations in the Baltic states think – and thereby undermine the integrity of elections in these states.[30]

Critically, this cognitive warfare strategy is an evolution of longstanding Russian strategy. As one US expert on Russian foreign policy noted, Russia's use of information operations to undermine political stability in Western states is "an old story that we are only recently rediscovering."[31] While the tools employed have changed, and the information environment itself has evolved, the strategy remains the same. At its core, what we see in the Baltic states is very similar to Soviet propaganda efforts during the Cold War. Russia today aims – as the Soviet Union once did – to divide Western societies and undermine their political institutions and broaden fissures between Western states, placing strain on NATO and the EU.[32] [33]

Russian Information Operations in the Baltic States

Russian information operations use disinformation, propaganda, and the selective release of politically-sensitive information to alter public opinion. Russia amplifies this information on social and traditional media to **exacerbate existing divisions in Estonian, Latvian, and Lithuanian societies and undermine their elections.** Rather than trying to create new divisions within these societies out of whole cloth, Russia takes advantage of the sensitive political, ethnic, social, and economic issues that already divide the populations of the Baltic states. "[I]t is always easier to do disinformation successfully if you include a little bit of the truth," said one government official with responsibility for hybrid threats.[34]

The recent Eesti 200 case is emblematic of how Russian information operations work in practice. A set of six posters appeared overnight at Hobujaama, a central tram stop in Tallinn, Estonia between Sunday, January 6 and Monday, January 7, 2019. As **Figure 4** shows, three of the posters read "Only Estonians here," (Siin Ainult Eestlased) the others read "Only Russians here," (Siin Ainult Venelased) with a column colored red separating the two sets – an explicit

Figure 4: The Eesti 200 Posters

Photo Credit: ERR News via Inga Kulmoja, University of Tartu

[30] **Note:** Surkov's ideas may find a historical antecedent in Edward Bernays, the founder of modern public relations, who wrote, "minds are molded, our tastes formed, our ideas suggested, largely by men we have never heard of." Edward Bernays (1928). *Propaganda*. Routledge.
[31] Interview with U.S. expert on Russian foreign policy, author interview, January 7, 2019.
[32] Ibid.
[33] Interview with U.S. expert on Russia and Europe, author phone interview, January 9, 2019.
[34] Interview with Latvian foreign affairs official, author interview, Riga, Latvia, January 18, 2019.

reference to policies of segregation.[35] The controversial posters were the work of Eesti 200, a liberal Estonian political party founded just a few months earlier. Intended to generate public interest in the party before the March 2019 parliamentary elections, the posters pointed to the ethnic divisions within the society between the Estonian majority and Russian minority – and a phone number directed interested citizens to a recording offering a message of unity, not division.[36] By Monday evening, Estonian news media were reporting that the posters had been covered up with advertising for a joint production by Tallinn's Russian and Estonian-language theaters.[37]

The saga of these posters – which were up for less than a day – demonstrates the efficiency of Russian efforts to exploit domestic divisions to undermine the integrity of elections in the Baltic states. As the posters began to get attention within Estonian society, with citizens posting pictures and commenting on them on social media, Russian state media jumped on the story and amplified it. Many channels, including Sputnik, Zvezda, Channel One (Первый канал), Russia Today, and Rossiya TV, called the posters a "scandal," and compared them to "apartheid in South Africa."[38] Coverage of the posters in Russian media – which is a significant source of news for many ethnic Russians in Estonia – built upon preexisting Russian narratives about discrimination against ethnic Russians and Russian-speakers in the country. Estonian officials confirmed to us that the speed and efficiency with which Russian actors repurposed the Eesti 200 posters for propaganda purposes was emblematic of Russian information operations.[39]

Russia uses information operations to affect public opinion in the Baltic states and ultimately weaken and divide these societies.

Eesti 200 is just one in a litany of cases of Russian disinformation campaigns targeting the political media and information ecosystem of the Baltic states we found during our research. These cases demonstrate Russia attempts to use information operations to affect public opinion in the Baltic states and ultimately weaken and divide these societies. Such efforts pose a serious threat to election integrity in these countries, as successful Russian campaigns to enflame political or social division with the aim of altering how voters think may result in election outcomes reflective – in part – of Russian preferences. Given that (as will be discussed below)

[35] Vahur Koorits, "Eestlased ja venelased saatis trammipeatuse eraldi nurkadesse Eesti 200," *Delfi*, January 7, 2019, https://www.delfi.ee/news/rk2019/uudised/eestlased-ja-venelased-saatis-trammipeatuse-eraldi-nurkadesse-eesti-200?id=84956185.
[36] Agaate Antson and Sander Punamae, "Estonia 200 provocative posters," *Postimees*, January 8, 2019, https://news.postimees.ee/6494099/estonia-200-provocative-posters.
[37] Matthew Luzmoore and Kalsa Alliksaar, "'Only Estonians Here': Outrage After Election Poster Campaign Singles Out Russian Minority," *Radio Free Europe/Radio Liberty*, January 10, 2019, https://www.rferl.org/a/estonia-election-posters-russian-minority-outrage/29702111.html.
[38] Ibid.
[39] Interview with Estonian strategic communications official, author interview, Tallinn, Estonia, January 16, 2019.

election systems in all the Baltic states are relatively secure, using cognitive warfare strategies to target the populations of the Baltic states – mainly ethnic Russian and Russian-speaking minority populations – is a lower cost, indirect way to affect political processes in their neighbors. "It is too expensive to hack our system," one Latvian official explained. "What [Russia] does instead is go after the population by media campaigns."[40]

Russian Information Tactics in the Baltic States

At the tactical level, the primary vector for Russian influence operations in the Baltic states is Russian-language media (often state-controlled). This includes both news that is broadcast domestically in Russia as well as to diaspora communities in the Baltic states – particularly on television – and Russian-language news sources in print and online. As one Latvian official told us, "we see what the Russians see."[41]

Russian-language media outlets in Estonia and Latvia demonstrate a clear preference for pro-Russia parties in the run-up to elections. Ahead of the parliamentary elections in Latvia in October 2018, Sputnik Latvia, Baltnews.lv and the Russian language portal of Delfi in Latvia overrepresented visually the Harmony Centre party (Saskana), which has close ties to Russia.[42] An analysis of Russian media coverage during the run-up to the Estonian parliamentary elections in March 2019 shows a similar pattern. The Center Party (Keskerakond), also a more Russia-friendly party, received considerably more positive coverage than any other parliamentary rivals.[43] Given that Russian language media is a significant source of news for the Russian-speaking populations of Estonia and Latvia, the importance of how political parties are represented on Russian television should not be understated – this is just one more way in which Russia seeks to undermine the integrity of elections in the Baltic states.

Other Forms of Malign Influence

The strategic use of information is not the only way that Russia tries to influence and undermine the politics of the Baltic states. Other vectors include efforts to suborn political parties, illicit Russian financial ties, and efforts to promote Russia-linked non-governmental organizations (NGOs). For example, in the Eastern Money Scandal, Estonia's intelligence services deemed Estonian Centre Party leader Edgar Savisaar an "agent of [Russian] influence" after he accepted millions in funds from Russia.[44] [45] Similarly, Latvia's Harmony Centre party is widely understood to have connections with Kremlin interests. And in Latvia's ABLV banking scandal, Russia non-residential depositors laundered money though one of Latvia's largest banks. The discovery of these illicit financial networks led to ABLV's closure in 2018. Before this, Russia-linked civil society organizations and NGOs such as Native

[40] Interview with Latvian foreign affairs official, author interview, Riga, Latvia, January 18, 2019.
[41] Interview with Latvian foreign affairs official, author interview, Riga, Latvia, January 18, 2019.
[42] Digital Forensic Research Lab, "#ElectionWatch: Graphic Preference from Russian Media in Latvia," *Atlantic Council*, September 24, 2018, https://medium.com/dfrlab/electionwatch-graphic-preference-from-russian-media-in-latvia-44853a34e9c4.
[43] "The Kremlin election compass," *Propastop*, February 19, 2019, https://www.propastop.org/eng/2019/02/19/the-kremlin-election-compass/.
[44] "A Political Scandal in Estonia and Russian Influence in the Baltics," *Stratfor*, December 27, 2010, https://worldview.stratfor.com/article/political-scandal-estonia-and-russian-influence-baltics.
[45] Interview with Estonian security official, author interview, Tallinn, Estonia, January 14, 2019.

Language, an organization that pushed for making Russian an official language in Latvia in 2012."[46] This is all not to mention traditional espionage, at which Russia is, of course, well-practiced.

Consistent Narratives at the Operational and Tactical Level

At the operational and tactical level, Russian information operations against the Baltic states **consistently emphasize three broad narratives**, as shown in Figure 5. According to the government officials and outside experts we spoke with, Russia's emphasis on these themes persisted over many years and is common across each of Estonia, Latvia, and Lithuania. While Russia tailors particular pieces of disinformation and propaganda to local circumstances, they remain within this outline.[47] Our interviews confirm that Russia views Russian ethnic minorities and Russian-speaking populations as a leverage point in the Baltic states. However, these populations do not generally favor separatism or union with Russia – to draw a parallel between the Russian minority populations in the Baltics and Russian compatriots in Crimea would be highly suspect.[48]

Figure 5: Narratives at the Operational and Tactical Level

The first narrative theme depicts the Estonian,

[46] Andrew Wilson, "Four Types of Russian Propaganda," *Aspen Review*, Issue 4 (2015), https://www.aspenreview.com/article/2017/four-types-of-russian-propaganda/.
[47] Interviews with military and foreign affairs experts, author interviews, Tallinn, Estonia, Riga, Latvia, and Vilnius, Lithuania, January 2019.
[48] "Ambiguous Threats and External Influences in the Baltic States: Phase 2: Assessing the Threat," *Asymmetric Operations Working Group* (November 2015), https://www.stratcomcoe.org/ambiguous-threats-and-external-influences-baltic-states, 43-44.

Latvian, and Lithuanian governments as **fascist or pro-Nazi.** A common refrain in Russian state media depictions of the Baltics, this set of themes is emblematic of the strain of Russian propaganda that appeals to and exploits historical memory, particularly among older generations and Russian populations. Officials tracking disinformation told us that these appeals regularly resurface around sensitive anniversaries, such as the annual Victory Day celebrations commemorating Soviet victory in World War II.[49] An incident emblematic of Russia's instrumentalization of historical memory is the controversy over the relocation of Soviet-era monuments – in this case, the Bronze Soldier of Tallinn (Pronkssõdur / Бронзовый Солдат). Russian state media widely covered the statue's relocation by the Estonian government in April 2007. The feverish coverage contributed to two nights of riots in Tallinn, a week-long siege of the Estonian embassy in Moscow, and, ultimately, Russian cyberattacks against Estonian government institutions, banks, and media organizations.[50]

The second narrative theme depicts Estonia, Latvia, and Lithuania as **flawed or failed states.** Russia-affiliated media and messages proliferated via social media regularly assert that the Baltic states are dysfunctional states with failing economies that are incapable of providing a good standard of living for their citizens. Additionally, these narratives tend to focus on Russia's defense of "traditional values," emphasizing the Baltics states' acceptance of Western standards on issues such as the treatment of LGBTQ+ people. Explicit comparisons to standards of living and values systems in Russia – in which Russia is falsely asserted to be more prosperous or otherwise preferable – are frequent as well. These narratives reflect Russia's strategy of seizing on divisive issues within societies and exacerbating them for political gain.

The third narrative theme claims that Estonia, Latvia, and Lithuania **discriminate against ethnic Russians, Russian-speakers, or non-citizens**. Putin has made the protection of and advocacy for Russian minority populations outside its borders a central component of Russian policy in recent years.[51] Russia is driving the process of, as one analyst put it, "diasporisation" throughout the former Soviet Union, pushing a narrative of collective Russian national or civilizational identity – the "Russian World" (Русский Мир).[52] In the Baltic states, the crux of this narrative is that Russia seeks to protect these populations while the governments of Estonia, Latvia, and Lithuania systematically discriminate against them. References to the status of the Russian language in the Baltic states are frequent, especially during moments – such as the 2012 Latvian constitutional referendum – when the status of Russian as an official language was a matter of public debate. The purpose of these narratives is to exacerbate existing grievances within the ethnic-Russian and Russian-speaking populations, divide the Baltic societies along ethnic and linguistic lines, and increase the salience of ethnic identity to bolster pro-Russian political forces.

[49] Interview with Lithuanian defense official, author interview, Vilnius, Lithuania, January 22, 2019.
[50] Andreas Schmidt, "The Estonian Cyberattacks," in *The fierce domain – conflicts in cyberspace 1986-2012*, ed. Jason Healey (Washington: Atlantic Council, 2013). https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks.
[51] Agnia Grigas, *Beyond Crimea: The New Russian Empire* (New Haven: Yale University Press, 2016), 57,75-7783-93.
[52] Kristina Kallas, "Claiming the diaspora: Russia's compatriot policy and its reception by Estonian-Russian population," *Journal on Ethnopolitics and Minority Issues in Europe*, Vol. 15, No. 3, (2016): 2-3, https://www.ecmi.de/fileadmin/downloads/publications/JEMIE/2016/Kallas.pdf.

Resilience and Immunity

Our conversations with officials in Tallinn, Riga, and Vilnius hit on two primary strategies for addressing the threat that Russian information operations pose to election integrity. The first includes efforts to tactically address the disinformation threat, such as by working with social media companies to identify and remove fake accounts or by debunking fake news. Such strategies were deemed to be helpful on a micro-scale, which given the small size of the Baltic states themselves made them attractive. However, to truly protect the integrity of elections and mitigate the impact of Russian information operations, a more robust second set of strategies that enhance societal resilience to Russian tactics is necessary.

A common refrain in all three Baltic capitals was that their populations have developed an immunity to Russian disinformation and propaganda that renders Russian information efforts ineffective. One Estonian member of parliament told us that "we have understood [disinformation] for many decades" and that the experience of Soviet occupation and propaganda made the society more resilient to Russian information operations today.[53]

Our assessment, however, is that the actual resilience or immunity of Baltic publics deserves a higher level of scrutiny. Our research in the Baltic capitals suggests that while the narrative of societal immunity remains common, it is likely an overestimation. Many interviews used public health analogies, speaking of public's "vaccination" against Russian disinformation. This point is still an open question. Looking to the future, we question the ability of susceptible populations in these states to discern Russian disinformation – which has become increasingly sophisticated in recent years – from legitimate news and public debate. As one Latvian expert on disinformation told us, "we can't call what we have true resilience. What we have here is a reflex."[54]

The principal concerns are the ethnic Russian and Russian-speaking populations. Officials indicated that these groups, which tend to consume Russian state-controlled media, are the most susceptible to Russian influence through those media channels. This phenomenon is particularly problematic in the case of older generations, for whom television (rather than social media) remains a primary source of news and entertainment. One Lithuanian official pointed to the common tactic on Russian-affiliated television of "sandwiching" propagandistic or misleading content between popular entertainment programs broadcast in the Baltic states.[55] Meanwhile, other officials and experts pointed to concerns about the susceptibility of younger generations. Young people tend to consume social media at higher rates but may lack the ability to detect fake news or Russia-authored content. A contributing factor to this occurs when ideas propagate through social networks based on popularity, rather than authority.[56] For example, Russian internet trolls insert disinformation that is amplified and spread by unwitting users.[57]

[53] Interview with Estonian politician, author interview, Tallinn, Estonia, January 15, 2019.
[54] Interview with Latvian disinformation expert, author interview, Riga, Latvia, January 18, 2019.
[55] Interview with Lithuanian military expert, author interview, Vilnius, Lithuania, January 23, 2019.
[56] Timothy P. McGeehan, "Countering Russian Disinformation," *Parameters*, 48(1), (U.S. Army War College, 2018), 55.
[57] April Glaser, "Reddit Is Finally Reckoning with How It Helped Spread Russian Propaganda in 2016," Slate, March 5, 2018.

Additionally, Russia regularly uses both fake accounts and bots to inject disinformation into the public discourse. The proliferation of online disinformation has escalated rapidly.

The issue, however, also extends beyond the Russian-speaking population. Interviewees in all three capitals were skeptical that any societal immunity to disinformation was extensive. While there was general agreement that their populations could distinguish explicitly pro-Russian content from unbiased news, their confidence did not extend to disinformation in other politically-sensitive areas not explicitly tied to Russia itself. One Latvian official told us that while their citizens have developed "some kind of immunity, it is by no means perfect, and people sometimes want their perceptions to be reinforced."[58] An outside expert on disinformation stated that the effectiveness of Russian information operations "is not about changing my beliefs, but about whether it speaks to my existing beliefs and can thus affect my behavior."[59]

On highly-divisive political issues, such as immigration, economic policy, language and ethnic politics, or even the legitimacy of elections, the populations of the Baltic states are likely susceptible to Russian information operations that seek to reaffirm and enflame their existing biases and perceptions. Moreover, Russia has recognized this vulnerability and is seeking to capitalize on it. Experts told us that while Russian information operations were in the past mostly directed towards the ethnic Russian populations, there has been a recent increase in appeals to the non-Russian population and particularly to individuals with far-right political leanings.[60]

Societal Trust During Election Periods

The threat to election integrity from Russian cognitive warfare efforts is clear. Russia targets vulnerable or susceptible populations within the Baltics states with the goal of affecting how voters think – and thus how they vote. Elections are the time at which democracies are most vulnerable to cognitive warfare operations. Our research in the Baltic states suggests that building and maintaining trust in government and the electoral system are vital to efforts to mitigate the effects of information operations on elections. Former Estonian President Toomas Hendrik Ilves called trust "crucial."[61] He writes: if "people do not trust their government, they will not trust voting systems either … security should not be seen as [an] excuse or an additional cost but as an enabler, guarding our entire digital way of life."[62] Russian information operations work to widen divisions within these societies and increase

"The Soviet Union's goal was to convince. Russia's goal is to confuse."

[58] Interview with Latvian foreign affairs official, author interview, January 21, 2019.
[59] Interview with international disinformation experts, author interview, Riga, Latvia, January 18, 2019.
[60] Interview with Estonian politician, author interview, Tallinn, Estonia, January 15, 2019.
[61] Toomas Henrik Ilves, "Foreward: Toomas Henrik Ilves, President of the Estonian Republic," in *E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015)*, eds. Mihkel Solvak and Krisjan Vassil (Tartu: Johann Skytte Institute of Political Science, University of Tartu, 2016), xiii.
[62] Ibid.

distrust in the government and the legitimacy of the political system as a whole. "The Soviet Union's goal was to convince. Russia's goal is to confuse," one Estonian official told us.

How do these governments build and maintain trust? Experts from Latvia, Lithuania, and Estonia emphasized the importance of avoiding sensationalism when communicating with the public. One Estonian official told us that they have found responding to disinformation with positive messages that reinforce core societal values to be much more effective than attacking or debunking.[63] Essentially, governments must act in ways to **safeguard political stability and trust in the political process** during the election period. Officials involved in monitoring disinformation similarly emphasized to us the importance of being strategic and careful in differentiating foreign interference from the legitimate and protected speech of political actors inside the country. As the same official told us: "freedom of speech doesn't only apply to positive messages."[64]

[63] Interview with Estonian strategic communications official, author interview, Tallinn, Estonia, January 16, 2019.
[64] Ibid.

The Cyber Threat to Election Integrity

- The probability of Russia successfully, undetectably hacking an election is low.
- Russia does not view cyberattacks against election systems as the most effective means of undermining the politics and institutions of Estonia, Latvia, and Lithuania.
- Russian cyber capabilities should be understood primarily as an enabler of information operations that undermine election integrity.
- Government networks and election systems are not the only targets – Russia routinely attacks the systems of political parties, campaigns, and other political actors.

Russia uses its offensive cyber capabilities to support efforts to undermine election integrity in Estonia, Latvia, and Lithuania. State-supported hackers target both governmental and non-governmental networks in these states. These cyber capabilities pose two distinct threats to election integrity:

1. Direct Technical Compromise of Voting Systems – including the threat of a cyberattack against digital components of election systems, including voting machines, vote tallying systems, voter databases, and election-night reporting systems. In the most extreme scenario, a successful Russian hack of voting systems could allow the Kremlin to alter vote tallies.
2. Cyberattacks that Enable Information Operations – including the use of cyber capabilities to support or otherwise enhance Russia's ongoing cognitive warfare and political interference efforts in the Baltic states.

Election Hacking: Low Probability, Medium Impact

Estonian, Latvian, and Lithuanian officials expressed confidence that they have successfully mitigated the risk posed by Russian efforts to compromise voting systems. Election and cybersecurity officials in all three countries expressed high confidence in their election security posture and assessed that the risk of successful, undetected Russian penetration of these systems was negligible. The confidence voting system security was evident in Estonia, which operates a digital-first elections system and allows for online voting, and Latvia and Lithuania, both of which employ a primarily paper-based system.

This confidence reflects a common underlying risk assessment: the three Baltic governments do not view the technical compromise of voting systems as the primary vector for Russian influence in their domestic politics. Instead, the Baltic governments view information operations and associated influence campaigns as the primary threat vector. While Russia works to influence election results and undermine the political systems of the Baltic states, efforts to hack into voting systems and change votes have not played a significant role in Russian strategy in the region. Instead, Moscow emphasizes the set of methods discussed in the previous chapter – disinformation, propaganda, and other forms of political interference.

To be clear, Estonia, Latvia, and Lithuania do not see the threat of technical compromise as nonexistent – nor do they treat it as such. Our conversations with officials involved in election administration, cybersecurity policy, and threat assessment suggest these governments take this risk quite seriously. All three governments prioritized the cybersecurity posture of their elections systems, developed procedures for monitoring the cyber threat to critical infrastructure systems, and established protocols for auditing elections results in the event of irregularities.[65]

Even so, they view a successful, undetected effort by Russian to alter vote tallies using cyber means as a comparatively low-probability event – especially when juxtaposed against the near-constant barrage of disinformation and subversion efforts directed against their political systems. They also recognize, as one cybersecurity official told us, that the adoption of digital technologies in the provision of government services and the conduct of elections inevitably introduces risk and cyber vulnerabilities that information security professionals must mitigate.[66]

Our research supports their assessment. While technical compromise of voting systems and related elections infrastructure is possible, we assess that Russia is unlikely to view cyberattacks against election systems as the most effective mechanism for advancing its political interests in the Baltic context. Notably, Russia does not appear to have targeted election systems during either the October 2018 Latvian parliamentary elections[67] [68] or the March 2019 Estonian parliamentary elections.[69]

The prevailing view among officials and outside experts was that while the risk of technical compromise exists, the absolute level of risk is quite low. Our interviewees in Tallinn, Riga, and Vilnius stated that Russia's likelihood of attempting to use cyber means to directly alter votes in their elections in the near term was negligible. More importantly, interviewees emphasized that even if the Russians were to alter votes successfully, the impact on the political orientation of their countries would likely be limited – or effectively mitigated by post-election auditing procedures.

Wrong Tool for the Job

Cyberattacks against elections infrastructure are not a tool well-suited to advancing Russia's goal of undermining the politics and institutions of their Baltic neighbors. The cybersecurity posture of all three Baltic states appears sufficiently robust to complicate, if not prevent, Russian efforts to compromise election systems. As one official told us, cyberattacks against election infrastructure are complex and challenging for Moscow to carry out successfully, offering a

[65] Estonian, Latvian, Lithuanian election and cybersecurity officials, author interviews, January 16, 21, 22, 2019.
[66] Interview with Estonian cybersecurity official, author interview, Tallinn, Estonia, January 15, 2019.
[67] Interview with Latvian election officials, author interview, Riga, Latvia, January 17, 2019; Interview with Latvian foreign affairs officials, author interviews, Riga, Latvia, January 18, 2019 and January 21, 2019; Interview with Latvian cybersecurity official, author interview, Riga, Latvia, January 21, 2019.
[68] Note**:** While Russian operators did not target election systems, they did aim at government institutions. See: Gederts Gelzis, "Latvia says Russia targeted its foreign and defense bodies with cyber attacks," *Reuters*, October 8, 2018, https://www.reuters.com/article/us-latvia-russia-cyber/latvia-says-russia-targeted-its-foreign-and-defense-bodies-with-cyber-attacks-idUSKCN1MI1SB.
[69] Interview with Estonian strategic communications official, author phone interview, March 22, 2019.

lower chance of success at a much higher cost when compared against other methods of political interference.[70] Additionally, it is unlikely that vote alterations of the magnitude necessary to change the balance of power in Tallinn, Riga, or Vilnius in a pro-Russia direction would not be detected by the preventative measures in place to catch irregularities.

While Russia has sought to improve the political standing of pro-Russian parties and politicians, doing so has not been the core of their approach. Indeed, as one Latvian official told us, Russia has mostly discarded such efforts, recognizing that elevating a pro-Russian party to power in Latvia is not possible in today's political environment.[71] While Harmony, a pro-Russian party, routinely wins the plurality of seats in the parliament, it has never been able to form a government – Latvia's other parties have always formed a coalition explicitly designed to leave Harmony in opposition.[72] Instead, Moscow has primarily used disinformation and targeted propaganda to pursue this aim, crafting and advancing narratives designed to exacerbate cleavages within society and undermine the politics and institutions of these states.

It is important to note one caveat. While efforts to directly alter votes using cyber means are not the most effective tool for advancing Russian interests, these types of attacks – even if ultimately unsuccessful – could be an integral part of Russia's broader disinformation strategy. Officials across all three governments told us that the instrumental value of a cyberattack by Russia would likely be in its effect on public trust in the electoral system and the government more broadly, not in its effect on vote tallies or election outcomes.[73] The chaos and dysfunction that a disinformation campaign alleging the compromise of election systems would produce could advance Russian interests much more than the alteration of a few votes.

Cyber as an Enabler of Information Operations

While officials described the risk of direct technical compromise of voting systems as low, they expressed deep concern about how cyber capabilities interface with and enable Russian information operations. Our assessment aligns with these concerns. Our research suggests that Russian cyber capabilities should be understood primarily as an enabler of other cognitive warfare operations. Cyber capabilities, while powerful, are not necessarily a direct threat to election integrity in the Baltic states. Cognitive warfare operations, however, can create chaos and uncertainty that serves Russian strategic interests. These operations would include disinformation, propaganda, and related subversion efforts to undermine election integrity.

The primary function of Russia's cyber capabilities within its political interference efforts against Western states has been to target and extract information from party organizations or campaign targets – not to attack voting systems directly. Russia uses its offensive cyber

[70] Interview with Latvian cybersecurity official, author interview, Riga, Latvia, January 21, 2019.
[71] Interview with Latvian foreign affairs official, author interview, Riga, Latvia, January 21, 2019.
[72] Vassilis Petsinis, "As long as it lasts: Latvia's new coalition government," *openDemocracy*, January 26, 2019, https://www.opendemocracy.net/en/can-europe-make-it/as-long-as-it-lasts-latvia-s-new-coalition-government/.
[73] Interview with Estonian election official, author interview, Tallinn, Estonia, January 15, 2019; Interview with Latvian election official, author interview, Riga, Latvia, January 17, 2019; and Interview with Lithuanian defense official, author interview, Vilnius, Lithuania, January 22, 2019.

capabilities to infiltrate the systems of politically-active individuals and organizations and to extract politically-sensitive information, which is then released strategically and amplified to disrupt or otherwise affect an election. As one expert on Russian strategy told us, in the Baltics "cyberattacks are followed by information attacks."[74]

Russia's real-world tactics support this assessment. In a 2019 report, the Estonian Foreign Intelligence Service assessed a serious Russian threat to the upcoming European parliamentary elections, stating that Russia supports its preferred parties and candidates by, in part, discrediting their opponents by "stealing and leaking internal information."[75] Kremlin hackers used similar tactics in both the 2016 U.S. presidential election[76] and the 2017 French presidential election,[77] stealing information from political campaigns and party organizations and then releasing it publicly to affect the election outcome.

Extraction of information is not the only way in which Russia's cyber capabilities enable its political interference operations. Cyber capabilities have also been integral to some of Russia's information operations in the Baltic states. Latvia's experience before its 2018 parliamentary elections underscores the interplay between cyber capabilities and information operations.

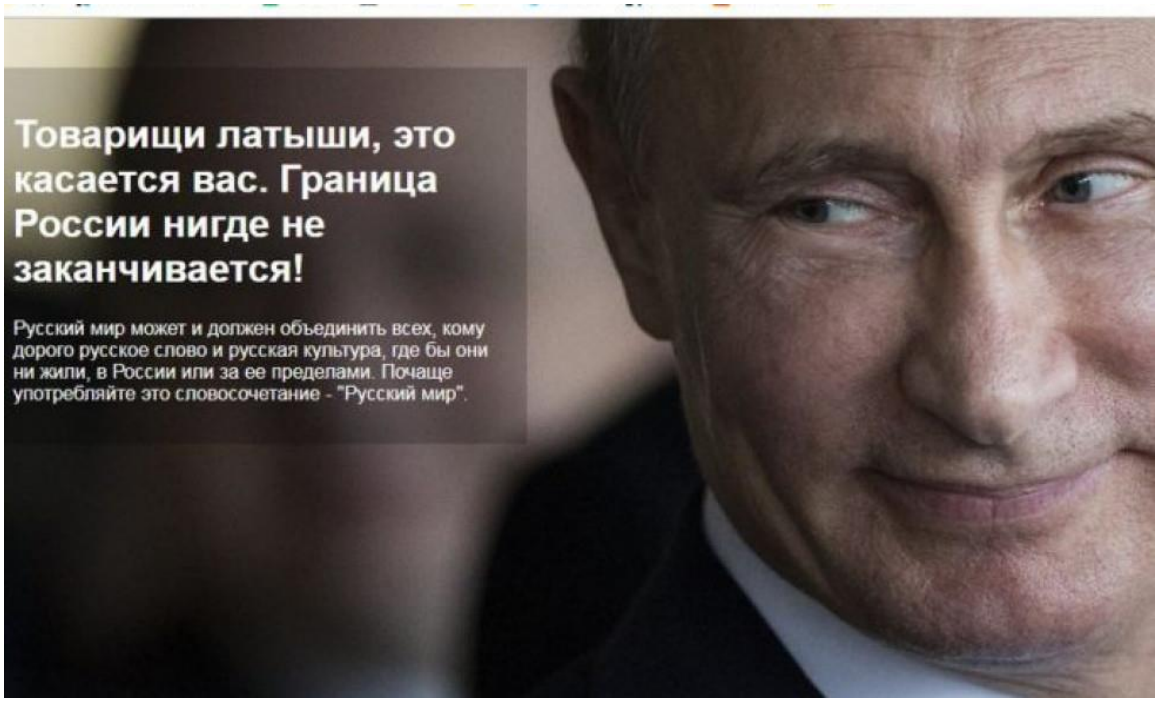
In September 2018, attackers targeted Delfi, the most popular news portal in Latvia, with a distributed denial of service (DDoS) attack just as it was preparing to broadcast the debate between the top candidates for Prime Minister.[78] On Latvia's election day, hackers infiltrated Draugiem.lv, a popular social network in Latvia, replacing the homepage with pro-Russian propaganda, images of Russian President Vladimir Putin, the Russian flag, and the Kremlin. As Figure 6 shows, these hackers issued a message on Draugiem.lv supporting Latvian separatism:

> Latvians, this concerns you. Russia's border never ends! The Russian world can and must unite everyone to whom the Russian language and culture is dear, no matter where they are, in Russia or beyond its borders. Use this phrase more often – "Russian world!"[79]

Both attacks are believed to have been conducted by either the Russian security services or by so-called "patriotic hackers" working on Moscow's behalf.[80]

[74] Interview with Estonian expert, author interview, Tallinn, Estonia, January 14, 2019.
[75] Estonian Foreign Intelligence Service, "International security and Estonia 2019," 2019, https://www.valisluureamet.ee/pdf/raport-2019-ENG-web.pdf, 41.
[76] "Intelligence Community Assessment," ii.
[77] Vilmer, "Successfully Countering Russian Electoral Interference."
[78] Interview with Latvian defense official, author interview, Riga, Latvia, January 18, 2019; and Interview with Latvian cybersecurity expert, author interview, Riga, Latvia, January 21, 2019.
[79] Author translation. See also: Digital Forensic Research Lab, "#ElectionWatch."
[80] The term "patriotic hackers" was coined by Russian President Vladimir Putin during a press availability in mid-2017. In response to questions about Russian hacking and political interference in the 2016 U.S. presidential election, Putin stated that "Hackers are free people [who may] read about something going on in interstate relations and if they have patriotic leanings, they may try to add their contribution to the fight against those who speak badly about Russia." He went on to note that it was "theoretically possible" that such patriotic hackers interfered in the U.S. election. For more information see: Krishnadev Calamur, "Putin Says 'Patriotic Hackers' May Have Targeted U.S. Election," *The Atlantic*, June 1, 2017, https://www.theatlantic.com/news/archive/2017/06/putin-russia-us-election/528825/; Nicu Popescu, "Russian cyber sins and storms," *European Council on Foreign Relations*, October 10, 2018, https://www.ecfr.eu/article/commentary_russian_cyber_sins_and_storms; and Daniil Turovsky, " 'It's our

Figure 6: The Hacked Draugiem.lv Homepage



Source: "In Latvia, a social network was hacked," FrontNews International, October 6, 2018, https://frontnews.eu/news/en/38121/In-Latvia-a-social-network-was-hacked-Putin-appears-on-the-opening-of-the-social-page-and-the-anthem-of-the-Russian-Federation-sounds.

In each case, an information operation designed to interfere with the electoral process took advantage of cyber vulnerabilities in non-governmental networks. Targeting such networks remained a core tactical element even as Russia's larger strategic emphasis shifted, with some attacks designed to limit opportunities for public debate and others designed to enflame ethnic and social tensions. While neither of these examples likely directly altered the election outcome, these attacks are emblematic of the methods used in Russia's cognitive warfare and political interference campaigns throughout the region. Offensive cyberattacks against vulnerable, politically-sensitive organizations and individuals enable many of Russia's information operations, furthering its broader goal of undermining the elections and political systems of the Baltic states.

time to serve the Motherland' How Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers," *Meduza.io*, August 7, 2018, https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland.

Recommendations for the Baltic States

Following our fieldwork, we concluded that most of the policies already implemented by the governments of the Baltic states were sound. Designed to safeguard election integrity and mitigate the impact of Russian disinformation, we see the current approaches of these governments as successful and worthy of continued investment and expansion. Therefore, several recommendations below expand on policies already implemented. Rather than try to reinvent the wheel, these recommendations seek to build upon the stable foundation already in place in Tallinn, Riga, and Vilnius. These recommendations are designed to enhance government effectiveness in responding to the threat to election integrity that Russia poses in the short-term and to promote improved societal resilience to cognitive warfare operations over the long-term.

We have included in Appendix 4 an analysis of our recommendations judged against the criteria for evaluation that we used for this project.

Recommendations for all Three Baltic States

1. Expand Investments in Election Cybersecurity
2. Provide Additional Resources to Working Groups on Election Security, Disinformation, and Strategic Communications
3. Exercise and Stress-Test Contingency Plans
4. Deepen Sharing of Intelligence, Best Practices, and Lessons Learned
5. Invest in Monitoring and Explore Regulatory Approaches
6. Expand Integration Policies Targeting Russian Minority Populations
7. Craft and Promote Compelling, Unifying National Narratives

Estonia-specific Recommendations (See Appendix 4)

1. Appropriate Funding for a Disinformation Public Education Campaign
2. Improve Quality of Programming and Funding for ETV+

Latvia-specific Recommendations (See Appendix 4)

1. Promote citizen fact-checking and investigative journalism
2. Appropriate Funding for a Disinformation Public Education Campaign
3. National Narrative Campaign
4. Increase Military and Police Engagements with the Russian minority

Lithuania-specific Recommendations (See Appendix 4)

1. Formalize Elections Security Planning
2. Improve Translation of Lithuanian News into Russian on Public Television

Recommendation 1: Expand Investments in Election Cybersecurity

While we assess that the technical compromise of elections systems is not the primary vector through which Russia undermines election integrity in the Baltic states, this does not mean that the Baltic governments should be complacent with regards to securing their elections systems. On the contrary, enhancing the security of digital elections infrastructure should remain a priority throughout the region. Government departments with responsibilities for securing digital infrastructure should continue to monitor these systems, conduct penetration testing, and enhance the cybersecurity posture where appropriate. Our conversations in these capitals suggest that cybersecurity and election experts are focused on this issue and that their governments are committed to ensuring that the digital aspects of election systems – not to mention other federal government networks – remain defended against foreign compromise.

We also recommend that these governments take steps to enhance cybersecurity protections for non-government networks – particularly those of political parties, campaigns, and media organizations. Our analysis suggests that these networks represent an emerging threat vector integral to Russian information operations in the Baltic states.[81] [82] Cybersecurity protections at the campaign and party level often fall woefully behind those at the federal level, creating a security vacuum that Russian hackers can easily exploit. [83] All three governments currently offer seminars that advise campaigns on proper cybersecurity hygiene. Additionally, CERT teams and other government cybersecurity professionals have offered – on a voluntary basis – to assess or penetration test sensitive systems, such as email and web servers. Our interviews show that parties and campaigns have, for the most part, welcomed this assistance.[84] [85] [86] While these governments cannot extend full cybersecurity protections to these networks, we recommend that they expand their engagement with parties, campaigns, or media organizations, to encourage a more robust cybersecurity posture to defend against hacking efforts.

Recommendation 2: Provide Additional Resources to Working Groups on Election Security, Disinformation, and Strategic Communications

All three governments have developed departments or working groups focused on the issues of election security, strategic communications, and countering Russian information operations and disinformation. Our conversations with officials involved in these efforts suggest that they have been effective in bringing together different agencies to focus on both the technical and

[81] Interview with Lithuanian military expert, author interview, Vilnius, Lithuania, January 23, 2019.
[82] Erik Brattberg and Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* (Washington: *Carnegie Endowment for International Peace*, May 2018), https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf, 4.
[83] Robby Mook and Matt Rhoades, Cybersecurity Campaign Playbook: European Edition (Cambridge, MA: Belfer Center for Science and International Affairs, 2018), https://www.belfercenter.org/sites/default/files/files/publication/EuropeanCampaignPlaybook.pdf, 6-8.
[84] Interview with Estonian cybersecurity official, author interview, Tallinn, Estonia, January 16, 2019.
[85] Interview with Latvian cybersecurity official, author interview, Riga, Latvia, January 21, 2019.
[86] Interview with Lithuanian cybersecurity officials, author interview, Vilnius Lithuania, January 22, 2019.

information threats to their elections. However, these formats have been largely ad hoc in nature, convened in the periods around elections.

We recommend that the governments of Estonia, Latvia, and Lithuania formalize and increase the dedication of resources towards election- and disinformation-focused working groups, building up well-staffed, permanent bodies responsible for coordinating interagency contingency planning for, monitoring of, and response to threats to election integrity. In addition to a small permanent staff, these bodies should include representatives from all the relevant agencies (such as election commissions, ministries of foreign affairs and defense, CERT teams, and the intelligence services), with clear divisions of labor established between them. As one official involved in these ad hoc working groups told us, "when everybody deals with everything, nobody deals with anything."[87]

Finally, we recommend that these groups be explicitly non-political in nature, staffed to the degree possible by career civil servants rather than political appointees. These working groups must be trusted by the public to oversee elections and provide information in a non-partisan manner. Separating them as far as possible from partisan political interests is essential to building that trust. In Estonia, Latvia, and Lithuania, these bodies have fallen under either the Government Office or State Chancellery; we assess that both are suitable models.

Some officials expressed skepticism of the need for permanent bodies focused on election issues separate from the existing election commissions and ad hoc working groups. They pointed to the infrequency of elections as a justification, stating that ad hoc bodies convened during election periods were sufficient.[88] One official said that as long as the contingency planning for and structure of the ad hoc groups were in place, no permanent body would be necessary.[89] While we understand this perspective, we assess that the benefits of a permanent staff focused on cybersecurity, counter-disinformation, and strategic communications around election issues outweigh the costs. Building up a small, dedicated staff to lead on these issues will have three principal benefits: it will (1) improve government coordination, (2) build knowledge on the topic, and (3) strengthen the government's ability to deal with a real election integrity crisis.

Recommendation 3: Exercise and Stress-Test Contingency Plans

Conducting exercises and simulations to stress-test government contingency plans for election-related crisis scenarios is essential. The Baltic governments have all considered exercises, but they have not yet taken place.[90] [91] We assess that it is vital for these governments to make sure that the contingency plans they have developed "on paper" actually work in practice – the first time governments use these plans should not be in response to a real-world crisis. Exercises should focus on the full slate of threats to election integrity – cyber incidents and disinformation campaigns first and foremost.

87 Interview with Estonian strategic communications official, author phone interview, March 22, 2019.
88 Interview with Latvian cybersecurity official, author interview, Riga, Latvia, January 21, 2019.
89 Interview with Estonian strategic communications official, author phone interview, March 22, 2019.
90 Interview with Lithuanian crisis management officials, author interview, Vilnius Lithuania, January 24, 2019.
91 Interview with Estonian strategic communications official, author interview, Tallinn, Estonia, January 16, 2019.

We recommend that the Baltic governments hold election-focused tabletop exercises and stress-tests on a cycle tied to their upcoming elections. An exercise conducted six-to-nine months in advance of the election date, for example, would provide ample time for agency leaders to incorporate lessons learned into revised plans for election-day administration and crisis-related contingencies. Responsibility for coordinating and planning these exercises would ideally fall to the permanent election-focused bodies recommended above; in their absence, existing ad hoc working groups or the election commissions should coordinate.

These exercises also offer an opportunity for Estonia, Latvia, and Lithuania to expand partnerships with the US and other allies on improvements to election and information security. While joint election security exercises are of course not feasible (elections are a solely domestic activity), exercises and simulations can be a vehicle through which to expand collaboration and share best practices. We recommend that the Baltic states explore bringing foreign observers to domestic exercises/simulations on a reciprocal basis, expanding on existing election observations initiatives. We recommend beginning internal to the Baltic region itself and then expanding the roster of participants out to include elections officials from other European allies and the US. One particularly fruitful avenue for engagement is to build upon the existing state partnerships that Estonia, Latvia, and Lithuania have with Maryland, Michigan, and Pennsylvania, respectively, in the defense space.[92] Engagement on elections issues with U.S. state and local governments offers better prospects than attempts to engage with the federal bureaucracy, as elections in the US are administered at the state and local level.

Recommendation 4: Deepen Sharing of Intelligence, Best Practices, and Lessons Learned

Across our interviews, government officials and experts emphasized the importance of intelligence cooperation for understanding and responding to the Russian threat to election integrity.[93] Our interviews suggested that existing intelligence-sharing arrangements at the regional, bilateral, and EU/NATO levels currently work quite well. However, officials also indicated that there is significant room for improvement in mechanisms for engagement, cooperation, and intel-sharing specifically focused on election security issues and the threat posed by information operations and Russian disinformation.

Rather than invest time and resources into the development of new mechanisms of intergovernmental engagement on these issues, the Baltic states should work with allies to enhance the effectiveness of promising (but underperforming) multilateral formats that already exist. Several venues exist at the EU/NATO level operating in parallel to a veritable alphabet soup of international bodies and bilateral or multilateral formats.[94] As one Estonian official told

[92] "FACT SHEET: The United States and Estonia, Latvia, and Lithuania – NATO Allies and Global Partners," *U.S. Embassy in Latvia*, August 23, 2016, https://lv.usembassy.gov/u-s-baltic-summit-readout-2/?_ga=2.34192161.181103584.1554039661-239102275.1554039661.

[93] Interview with Estonian defense official, author interview, Tallinn, Estonia, January 15, 2019; Interview with Latvian defense and foreign affairs officials, author interviews, Riga, Latvia, January 18-21, 2019; and Interviews with Lithuanian cybersecurity and defense officials, author interviews, Vilnius, Lithuania, January 22, 2019.

[94] Interview with Latvian foreign affairs official, author interview, Riga, Latvia, January 18, 2019.

us, "a lot has been promised on paper. We now need to make it work in practice."[95] A crucial battle will be raising the prominence of these issues at NATO and the EU. Many Baltic officials told us that their allies have been slow to recognize the threat Russia poses, but that through persistent coalition diplomacy they have been effective in elevating the issue.[96] [97] [98]

We recommend that Estonia, Latvia, and Lithuania continue their coalition diplomacy and work selectively with like-minded governments to elevate issues of election cybersecurity and the Russian information threat at the international level. The EU is best suited for international policy planning on the topics of disinformation and election integrity. The EU previously called for improved detection, coordinated responses and increased public awareness to reduce the malign effects of disinformation.[99] Additionally, the EU requested member states implement the of Code of Practice on Disinformation, a series of self-regulatory standards to address the spread of online disinformation and fake news.[100] Specifically, military, diplomatic, and intelligence professionals from the Baltic states can add value to the EU conversation primarily through Pillar 4 of the EU's Action Plan Against Disinformation which speaks to raising awareness and improving societal resilience.[101]

Recommendation 5: Invest in Monitoring and Explore Regulatory Approaches

The governments of Estonia, Latvia, and Lithuania should explore regulatory and legal measures to counteract Russian propaganda and disinformation distributed via both traditional media and on social platforms. Such approaches may include greater enforcement of existing domestic legislation on media, the development of new regulations governing traditional media, and the direct regulation of social media companies to prevent the proliferation of disinformation on their platforms. One proposed reform is to require all political advertising on social media to plainly disclose its source of funding. However, this constitutes only the tip of the plausible regulatory iceberg.

We also recommend that Estonia, Latvia, and Lithuania push for regulatory approaches at the international level – mainly through the EU. The EU is currently leading on regulation in the digital and information spheres through the General Data Protection Regulation (GDPR). The European level offers the best opportunity for the Baltic states to craft regulations to mitigate the impact of Russian disinformation campaigns on both traditional and new media.

Finally, we recommend that these governments build up efforts to monitor their domestic information environments for Russian disinformation and propaganda. Our interviews suggest

[95] Interview with Estonian strategic communications official, author interview, Tallinn, Estonia, January 16, 2019.
[96] Interview with Estonian foreign affairs official, author interview, Tallinn, Estonia, January 15, 2019.
[97] Interview with Latvian cybersecurity official and foreign affairs official, author interviews, Riga, Latvia, January 18, 2019.
[98] Interview with Lithuanian defense officials, author interview, Vilnius, Lithuania, January 22, 2019.
[99] Naja Bentzen, "Online disinformation and the EU's response," *European Parliamentary Research Service*, 2019, http://www.europarl.europa.eu/RegData/etudes/ATAG/2018/620230/EPRS_ATA(2018)620230_EN.pdf.
[100] "Code of Practice on Disinformation," *European Commission*, September 26, 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation
[101] "Action Plan against Disinformation," *European Commission*, December 5, 2018, https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

that the mechanisms currently in place to track malicious activity on social and traditional media work well, allowing the governments to identify (if not always prevent) Russia-linked disinformation campaigns.[102] Building upon that foundation, the Baltic governments should couple their efforts to track disinformation independently with an expansion of their collaborations with the major social media platforms.

It is important to note one caveat here. While we see building regulatory approaches and monitoring regimes as a necessary part of any counter cognitive warfare strategy, governments must do so consistent with existing national legislation and constitutional provisions regarding freedom of speech.[103] For this reason, each of Estonia, Latvia, and Lithuania will follow a separate path with regards to regulations and monitoring. We are thus not offering a specific set of common regulatory recommendations.

Recommendation 6: Expand Integration Policies Targeting Russian Minority Populations

Ethnic Russian and Russian-speaking minority populations are the primary target of Russia's information operations designed to undermine the politics and institutions of the Baltic states. These groups – more numerous in Estonia and Latvian than in Lithuania – are more likely to regularly consume news and other media affiliated with or controlled by the Russian state, which serves as a channel for disinformation and propaganda. Additionally, these populations tend to be, on average, less integrated into political, social, and economic life, with significant subsets of the population feeling disaffected or marginalized within the society.[104] [105] While not a universal problem, the fact remains that Russia has identified these groups as a vulnerability to be exploited, explicitly targeting Russian populations with information operations designed to widen existing fissures in the society. Any comprehensive approach to combating Russian cognitive warfare in the Baltic states therefore needs to address these populations and their concerns.

We recommend that the governments of Estonia and Latvia substantially increase their investment in policies that seek to further integrate these minority groups into the broader society. Many programs already exist. However, officials and experts with whom we spoke stated that much work remains to be done. As one official told us, the government's goal should be to further "convince people that they have a stake in this country."[106] Governments should expand funding for and involvement in integration programs, partnering with non-governmental groups.

Governments should focus their programs in two specific areas. First, policymakers should prioritize integration programs targeting young Russian and Russian-speaking populations. As one expert noted, youth populations tend to face disproportionate difficulties in the labor market and struggle to find high-paid work in rural or semi-urban areas.[107] Additionally, policymakers in

[102] Interview with Lithuanian defense official, author interview, Vilnius, Lithuania, January 22, 2019.
[103] Interview with Estonian strategic communications official, author phone interview, March 22, 2019
[104] Interview with Estonian expert, author interview, Tallinn, Estonia, January 14, 2019.
[105] Interview with Latvian foreign affairs official, author interview, Riga, Latvia, January 21, 2019.
[106] Interview with Latvian foreign affairs official, author interview, Riga, Latvia, January 21, 2019.
[107] Interview with Estonian expert, author interview, Tallinn, Estonia, January 14, 2019.

Estonia and Latvia must make efforts to address the status of non-citizens. In Estonia and Latvia, non-citizens cannot vote or run for political office, serve in the military, and have restrictions in the type of profession they can participate. A remedy to the non-citizen issue would remove a contributing factor to pro-Russia sentiment in the Baltic states, while also taking away a key Kremlin narrative theme.[108]

Second, the potential integration of these minority populations into the Russian state media ecosystem is a significant vulnerability for the Baltic states. Addressing this vulnerability requires investments in high-quality, compelling, unbiased programming. Therefore, we recommend the Baltic governments carefully and strategically expand funding for sources of unbiased news, information, and even entertainment programming. While the exact method will be subject to debate, we propose include promoting television or internet programming in the Estonian, Latvian, or Lithuanian language with Russian subtitles, supplemented by smaller strategic investments in Russian-language programming. While we concede the Baltic states will never be able to compete with the Kremlin on media financing, governments can invest in ways to improve the overall media ecosystem in the Baltic states. This recommendation also includes the endorsement of investments in journalistic education or exchange programs with the EU and US, strategic funding of licensing agreements for public television programming, and increased funding for civil society organizations devoted to digital research that identifies coordinated disinformation activity.

Recommendation 7: Craft and Promote Compelling, Unifying National Narratives

Our conversations with experts in Estonia, Latvia, and Lithuania consistently returned to a common theme: building societal resilient to Russian cognitive warfare campaigns requires more than just protecting election systems and debunking or regulating away disinformation and propaganda. It requires the development of a compelling, unifying national narrative that acts as a countervailing force to the false, divisive narrative pushed by the Kremlin. As one Estonian expert put it, "our national resilience should be based on our own story, strong national identity, and narrative."[109] A Lithuanian cybersecurity official similarly emphasized the centrality of a higher purpose: our goal is to "protect the way of life."[110] According to our interviewees, Russia succeeds only insofar as it can offer a more compelling narrative than that the Baltic states themselves. Many emphasized that positive messaging is much more effective in counteracting disinformation and propaganda than are reactive, negative, and combative responses.[111] [112]

We recommended that these governments work internally to develop or fine-tune their strategic communications strategies – bringing in outside consulting assistance where necessary – and build up personnel and resources dedicated to promoting that positive narrative or set of attitudes

[108] Indra Ekmanis, "The Non-Citizen Non-Question: Latvia Struggles to Leave Soviet Legacy Behind," *Foreign Policy Research Institute*, October 18, 2017, https://www.fpri.org/article/2017/10/non-citizen-non-question-latvia-struggles-leave-soviet-legacy-behind/
[109] Ibid.
[110] Interview with Lithuanian cybersecurity official, author interview, Vilnius, Lithuania, January 22, 2019.
[111] Interview with Estonian strategic communications official, author phone interview, March 22, 2019.
[112] Interview with Latvian foreign affairs official, author interview, Riga, Latvia, January 18, 2019.

with the public. This recommendation is partially tied to the issue of integration policies as well – a meaningful goal of any strategic communications strategy must be to craft a narrative that is inclusive of and appealing to all portions of the population.

Lessons for Western Democracies

- Russia's cognitive warfare strategy is the primary threat to election integrity in Western states, not direct Russian cyber interference on voting systems.
- Cognitive warfare relies on preexisting domestic divisions and vulnerabilities to function; as long as those divisions persist, so will the Russian threat to election integrity.
- Countering Russian information operation is a society-wide information challenge.
- Cybersecurity matters and should be prioritized, including by non-government actors – particularly political parties and campaigns – integral to electoral processes.
- Russia's election interference and cognitive warfare campaigns are a long-term threat that governments will need to manage.

What can the US and other Western democracies learn from the Baltic experience addressing the threat that Russian cognitive warfare poses to election integrity?

Many of the factors that make the Baltic states comparatively more vulnerable do not exist in the societies of their Western allies. There is no sizable ethnic-Russian population in the US eager to engage with Russian nationalist narratives put forward by the Kremlin. Russian state media does not penetrate France or Germany nearly to the degree that it does Estonia and Latvia. Moreover, while malign Russian economic and financial influence is rising in Europe,[113] politically-compromising financial ties between actors in the Baltic states and their Russian counterparts have characterized Baltic political and economic life for decades.[114] The Baltic states also have the benefit of being small, such that specific policies implemented by these governments may not be appropriate or scalable to the US or other larger European countries.[115]

Even so, the Baltic experience carries essential lessons for democracies on both sides of the Atlantic. The governments of Estonia, Latvia, and Lithuania have nearly three decades of experience on the frontlines of Russia's cognitive war against the West. **By studying the Baltic experience, we can better understand the contours of Russia's overall policy and strategy.** Analysts and researchers can better identify the operational vectors through which Russia tries to undermine the politics, elections, and institutions of its adversaries, and stress test – in broad terms – the effectiveness of different policy approaches.

Lesson 1: Cognitive Warfare is the Primary Threat

Russia's cognitive warfare strategy and information operations are the primary threat to election integrity in Western states. While cyberattacks against elections systems and the prospect of

[113] Heather A. Conley, Donatienne Ruy, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook 2*, (Washington: Center for Strategic and International Studies, 2019), https://www.csis.org/features/kremlin-playbook-2.

[114] Interview with Lithuanian expert on Russia, author interview, Vilnius, Lithuania, January 23, 2019.

[115] As one Estonian official told us, the small size of the Baltic states often helps when crafting policy approaches. For example, Estonian officials say it is more feasible to monitor social media activity in a society of a few million than in a society the size of the US. Source: Interview with Estonian government official, author interview, Tallinn, Estonia, January 16, 2019.

Russia directly altering votes is – and should be – a significant concern for many governments, the threat remains as of this writing mostly hypothetical.

Responding to Russia's cognitive warfare is a gargantuan task. The breadth of Russian information operations is vast, and their target is not merely an election system but rather the society as a whole. Vladislav Surkov, a close advisor to Russian President Vladimir Putin and the architect of his domestic propaganda operation, recently wrote that:

> Foreign politicians talk about Russia's interference in elections and referendums around the world. In fact, the matter is even more serious: Russia interferes in your brains, we change your conscience, and there is nothing you can do about it.[116]

Our analysis of the Baltic experience suggests that Surkov is partially right. Russia identifies the existing social, political, and cultural fissures within Western societies and weaponizes them, seeking to undermine the integrity of elections and political processes by altering popular sentiment in ways that benefit Russia.

In the Baltic states, this often manifests as disinformation designed to enflame fissures between ethnic Russians and the state, or propaganda claiming that the Baltics are failed states. Elsewhere in the West, the manifestations of this strategy are different – a focus on racial politics in the US[117] or efforts to enflame anti-EU sentiment in the United Kingdom.[118]

Wherever Russia deploys cognitive warfare, the core of the strategy has remained the same. **The Kremlin's goal is to interfere in our minds and to change not just how voters vote but how voters think. Cognitive warfare weaponizes information and takes advantage of the existing fissures in Western societies to achieve a political end.** Russia uses the open media environments in Western states to turn our preexisting domestic vulnerabilities against us, undermining the integrity of our elections and destabilizing our political systems.

The implications for the U.S. and governments throughout Europe are clear. Improving the physical and cyber- security of election systems is an essential but insufficient response to the threat Russia poses to election integrity. Ensuring election commissions count votes accurately and securely transmit tallies does not address the threat posed by information operations designed to affect political sentiment or undermine trust in the political system.

In the Baltic states, Russia has sought to achieve its political aims without directly altering votes or compromising voting systems. From Russia's perspective, the goal is to weaken, divide, and distract an adversary to make them less capable of countering Russian interests at home or internationally. Chaos, instability, and domestic political division – in the Baltics, in the US, or in Europe – serve Russia's interests. Moreover, information operations offer the prospect of

[116] Surkov, "Долгое государство Путина;" and Maza, "Vladimir Putin's Adviser Tells Americans."
[117] Scott Shane, "These Are the Ads Russia Bought on Facebook in 2016," *The New York Times*, November 1, 2017, https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html.
[118] Patrick Wintour, "Russian bid to influence Brexit vote detailed in new US Senate report," *The Guardian*, January 10, 2018, https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report.

achieving these outcomes at a lesser cost and much lower risk of blowback than efforts to directly interfere with voting systems.

Lesson 2: A Society-Wide Information Challenge

While Surkov and his allies in the Kremlin are correct about the threat that cognitive warfare poses, in another respect they are gravely mistaken: **We *can* do something about it**. If the experience of Estonia, Latvia, and Lithuania over the last three decades shows us anything, it is that Western governments *can* mitigate the effects of Russian cognitive warfare. Responding to the threat of Russian information operations to election integrity is a long-term, society-wide information challenge. Doing so effectively requires a whole-of-government approach.

Our interviews in the Baltic states suggest three of the most common approaches include debunking Russian disinformation, increasing media literacy, and protecting election systems from cyber intrusion. We assess that these approaches are all helpful (and should be pursued) in the short-term. At the same time, the policy approaches alone are insufficient to mitigate the effects of Russian cognitive warfare over the long-term.[119] As one senior Latvian official told us, the scope of the challenge is much broader – at its core, cognitive warfare represents Russia "exploiting a fundamental shift in how our democracies function." Political discourse is increasingly relegated to unregulated, unmoderated spaces and platforms that often "naturally promote disinformation"[120] – a fertile environment for a cognitive warfare strategy to take hold.

When Russian cognitive warfare campaigns succeed, they do so because the narrative that Russia puts forward is more compelling to subsets of the population than the alternatives offered by the state or society itself. Cognitive warfare flourishes in political systems where trust in government is low, where social fissures divide people along deep ethnic, political, economic, social or cultural lines, and where large portions of the population feel disconnected from the state and their fellow citizens. Russian disinformation and propaganda campaigns are effective when they reinforce it reinforces existing views, prejudices, and biases within the target society.

> "[Russia] is exploiting a fundamental shift in how our democracies function."

The challenge facing the Baltic states and their Western counterparts is therefore to find policy solutions that increase societal resilience to Russian cognitive warfare efforts – that build, as several interviewees termed it, "cognitive security."[121] Central to this task are policy efforts that increase trust in core democratic institutions – election systems, unbiased media, and the government itself – and put forward a compelling, inclusive national narrative. Western governments should increase their strategic communications capacity, creating and empowering nonpartisan bodies responsible for monitoring, overseeing, and verifying the integrity of

[119] Interview with international disinformation experts, author interview, Riga, Latvia, January 18, 2019.
[120] Interview with Latvian foreign affairs official, author interview, Riga, Latvia, January 21, 2019.
[121] Ibid; interview with international disinformation experts, author interview, Riga, Latvia, January 18, 2019.

elections and communicating accurate, timely, and unbiased information to the public. So too should they focus on regulating more stringently the involvement of foreign actors in their political processes and the injection of state-sponsored news and opinion into the domestic political discourse, particularly on social platforms.

Finally, Western states must recognize that responding to and mitigating the impact of cognitive warfare on election integrity is not merely a technical challenge. On the contrary, as one expert told us, "the human aspect is 99 percent of the problem."[122] As such, Western states should prioritize identifying the populations that are at high risk of susceptibility to Russian disinformation and the vulnerabilities in their domestic information environments that make information operations possible. On this basis, they should design long-term policy interventions that seek to pull out the vulnerabilities at their root, addressing the legitimate grievances and concerns of vulnerable or disaffected populations within their societies and promoting trust in

Building societies more resilient to Russian cognitive warfare will be neither quick nor easy; it will be the work of decades, not years.

government and national unity. Estonian and Latvian efforts to better integrate the ethnic Russian and Russian-speaking minorities are examples of this type of policy approach, as these communities are all too often the target of Russian information operations.

We recognize that advising Western governments to mitigate the impact of Russian election interference efforts by bridging the gaps that divide their societies sounds grandiose and farfetched. However, we also must be clear-eyed in recognizing that **Russia's strategy of cognitive warfare relies on these very same domestic vulnerabilities to function – and that the threat to election integrity will not be fully mitigated as long as these vulnerabilities persist**. Russia did not create these fissures – it only seeks to exacerbate and enflame them to divide the West and advance its political interests. Building societies more resilient to Russian cognitive warfare will be neither quick nor easy; it will be the work of decades, not years.

Lesson 3: Cybersecurity Matters – For More Than Just Government

While we assess that the cyber threat to voting systems is not the primary vector through which Russia undermines election integrity in Western states, governments must continue to improve their cybersecurity posture. Western governments should address the threat of Russian cyberattacks against elections infrastructure through increased cybersecurity protections for elections systems. So too should Western governments work to improve the cybersecurity

[122] Interview with international disinformation experts, author interview, Riga, Latvia, January 18, 2019.

protections afforded to all government networks. Election systems are by no means the only likely targets of Russian cyberattack and cyberespionage. These steps are neither radical nor controversial. Indeed, the Russian cyber threat is on the radars of governments on both sides of the Atlantic, and nearly all have developed plans in recent years to improve their cybersecurity posture.[123]

Government networks, however, are not the only networks that matter. Russian cognitive warfare campaigns regularly make use of politically-sensitive information stolen from actors central to the target political system that are not directly part of the government itself. Of particular concern are the networks of political campaigns and political party organizations. Political campaigns are increasingly digital in nature; however, campaigns and political parties often lack the resources and cybersecurity know-how to adequately protect their networks from malicious actors.[124] Information stolen from campaigns and parties can be used by Russia to disrupt public trust in the electoral process or affect public opinion – and ultimately voter behavior.

While political parties and campaigns are responsible for their own cybersecurity, governments should not stand idly by. As Estonia, Latvia, and Lithuania have all done successfully in recent years, other Western governments should develop policy approaches that extend federal cybersecurity expertise to non-federal networks on a voluntary basis. At a minimum, government security experts should conduct training exercises on cybersecurity best practices for campaigns and parties and offer to advise these groups on how to establish secure networks. A more expansive set of government actions could include government assistance in penetration testing critical servers and networks, as has been done successfully in Latvia[125] and Lithuania.[126] While it would be inappropriate to extend federal cybersecurity protections to non-government networks, Western governments need to take a more holistic view of what digital systems are essential to the conduct of an election and take steps to protect more than just voting systems.

[123] A few notable examples include the "National Cyber Strategy of the United States of America," released in September 2018, the "French National Digital Security Strategy," implemented in 2015, and the "Cyber Security Strategy for Germany," implemented in 2016. All EU member states have developed a National Cyber Security Strategy. See: "National Cyber Security Strategies," *European Union Agency for Network and Information Security (ENISA)*, 2019, accessed March 14, 2019, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map; "National Cyber Strategy of the United States of America," *The White House*, September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; "French National Digital Security Strategy," *Premier Ministre*, 2015, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/information-systems-defence-and-security-frances-strategy; and "German National Cyber Security Strategy," *Federal Ministry of the Interior*, 2011, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-for-germany/view.

[124] Eric Rosenbach, Robbie Mook, and Matthew Rhoades, *The Cybersecurity Campaign Playbook* (Cambridge, MA: Belfer Center for Science and International Affairs, November 2017), https://www.belfercenter.org/publication/cybersecurity-campaign-playbook, p. 5-8.

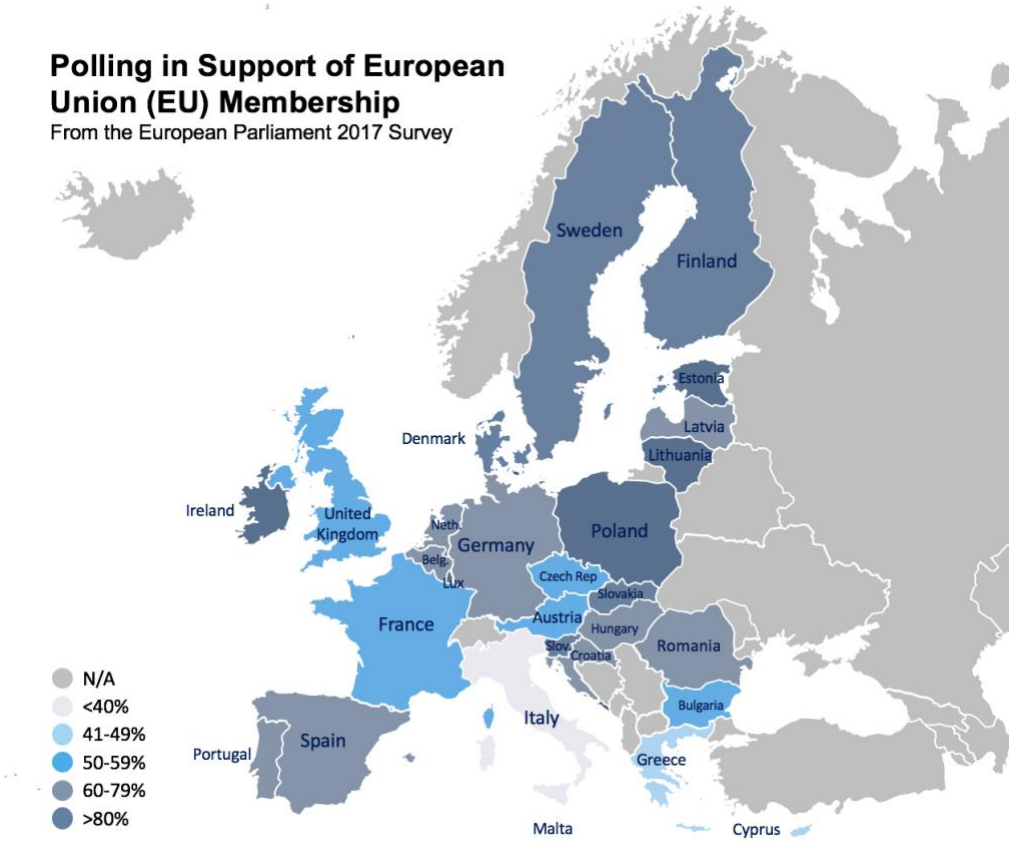
[125] Interview with Latvian cybersecurity official, author interview, Riga, Latvia, January 21, 2019.

[126] Interview with Lithuanian cybersecurity experts, author interview, Vilnius, Lithuania, January 22, 2019.

Lesson 4: Cognitive Warfare is a Persistent, Long-Term Threat

We assess that **cognitive warfare will remain a persistent threat to Western political systems over the medium- to long-term.** Operations targeting elections are but a manifestation of this broader strategy through which Russia seeks to undermine and divide its Western adversaries.[127] The underlying drivers of Russian grand strategy that caused Moscow to adopt this confrontational stance and set of asymmetric tactics are unlikely to change in the short- to medium-term. As such, we project that Russia will continue to engage in the types of cognitive warfare operations outlined in this report in both the Baltic states and other Western countries.

Figure 7: Support for the EU Throughout Europe



While we cannot say with certainty where Russia will strike next, we assess that the most significant and likely near-term targets are in Europe and the US. Russia is far and away the most frequent actor in foreign-influence efforts, conducting at least 38 distinct influence campaigns targeting 19 different countries, according to a Princeton University study.[128] In this sample of foreign influence efforts identified, about 38 percent targeted the US, 9 percent targeted the UK,

[127] Helmus, et al, "Russian Social Media Influence."
[128] Arya Goel, Diego Martin and Jacob Shapiro, "Managing and Mitigating Foreign Election Interference," *Lawfare*, July 21, 2019, https://www.lawfareblog.com/managing-and-mitigating-foreign-election-interference

and 6 percent targeted Germany.[129] The rise of populist and anti-EU parties within European states, and the underlying social and economic divisions that they have brought to the fore is of particular relevance.

As Figure 7 shows, support for European institutions in flagging across much of the continent – France, Italy, Greece, and others are experiencing high levels of societal dissatisfaction and anger. These divisions are tailor-made for exploitation by information operations designed to sow chaos, reduce faith in institutions, and change how voters vote. They present Moscow with an appealing target set, and we expect that Russia may well turn its attention to undermining the integrity of elections throughout Europe over the months and years to come.

On a broader level, however, Western governments must recognize that election interference and cognitive warfare operations will continue to pose a threat so long as their societies remain riven by profound political, economic, and socio-cultural divisions. While Russia cannot foment division itself, it can capitalize on it, exacerbating existing issues within Western societies in order to undermine them. And when the Kremlin looks at the West, it sees many – too many – attractive targets. Building up resilience to these tactics and mitigating their impact is a long-term challenge, one that Western governments will be grappling with for the foreseeable future. They should start now.

[129] Ibid.

Appendix 1: Interviews in the Baltic States and the US

We conducted in-person and phone interviews with government officials and experts in the United States and Europe. Our fieldwork consisted of nine days of meetings in the three Baltic capitals: Tallinn, Estonia; Riga, Latvia; and Vilnius, Lithuania. We listed only the institution and, where appropriate, the number of officials or experts we met with greater than one for each interviewee or set of interviewees. As discussed in the Methodology section, our interviewees opted to remain anonymous for candor on sensitive national security topics, and we are thus not releasing their names publicly in this appendix.

Estonia

E-Governance Academy (EGA), Electoral Office, Government Communications Unit of the Government Office, Kaitsepolitseiamet (Estonian Internal Security Service), Information Systems Authority, International Centre for Defense and Security (ICSD), Ministry of Defense, Ministry of Foreign Affairs (2), Riigikogu (Parliament)

Latvia

Central Election Commission, CERT.LV, Ministry of Defense, Ministry of Foreign Affairs (3)
NATO STRATCOMM Center of Excellence

Lithuania

Eastern Europe Studies Centre, Institute of International Relations and Political Science, Vilnius University, Military Academy of Lithuania (2), Ministry of Defense (6), Ministry of Foreign Affairs, Threat Management and Crisis Prevention Bureau (3), Vilnius Institute for Policy Analysis

United States

American Institute for Contemporary German Studies (AICGS), Belfer Center for Science and International Affairs, Harvard University (2), Center for Strategic and International Studies (CSIS) (2), Hoover Institution, Stanford University U.S. Department of State (6)

Appendix 2: Fieldwork Questionnaire

We used the templated questions below to structure our interviews. However, we asked additional questions and follow-ups during the natural flow of the conversations, in line with our semi-structured interview format. Additionally, we tailored our interview questions to the specific expertise of our interviewees. Not all of the below questions were asked during every interview. This list represents the foundation upon which more comprehensive, nuanced, and tailored conversations took place during our fieldwork.

1. How has Russia sought to undermine, affect, or otherwise alter the outcomes of elections in Estonia, Latvia, and Lithuania in recent years? What tools or capabilities have been used to do so?

2. What election security and related policies have Estonia, Latvia, and Lithuania implemented to counter Russian efforts or mitigate their impact?

3. What policies have Estonia, Latvia, and Lithuania implemented to combat Russian disinformation efforts, including efforts that target ethnic Russian or Russian-speaking populations?

4. What policy interventions could be implemented to further strengthen election security in Estonia, Latvia, and Lithuania?

5. What lessons or best practices from Estonia, Latvia, and Lithuania apply to elections in other contexts, including the United States?

6. What lessons from the United States or other alliance partners are applicable to the Baltic context?

7. How can Estonia, Latvia, Lithuania, and their alliance partners best promote engagement, cooperation, and information sharing on these issues?

8. Are current mechanisms/forums sufficient or will new modes of dialogue be necessary? What avenues and institutions can be leveraged to solve this issue?

9. What lessons in cybersecurity and counter-disinformation efforts from other contexts can be applied to the Baltic context? And what can other countries learn from the experience of Estonia, Latvia, and Lithuania?

10. What are the structural causes behind Russian aggression in the cyber and information spheres? Is there any policy that can reduce this aggression? Is cooperation or engagement with Russia possible in a bilateral or multilateral setting?

Appendix 3: Country-Specific Policy Recommendations

In addition to the comprehensive recommendations common to all three Baltic states offered above, these country-specific recommendations offer policy options at an operational level for the governments of Estonia, Latvia, and Lithuania. Cost remains a significant consideration for the policies offered for all three governments. Also, some of these policies will likely face concerns with administrative feasibility or long-term sustainability. Still, this report concludes these are the kinds of programs and policies that can build up resilience and cognitive security for the population of the Baltic states to counter the malign effects of Russian cognitive warfare and information operations.

Recommendations for Estonia

1. **Increase Funding and Staffing for Strategic Communications**
   This report found Estonia possesses one of the best practices for countering information operations in its strategic communications initiatives, including the message discipline of government officials. The Strategic Communications office focuses on ensuring Estonian's align to seven key attitudes to build up the resiliency of the population from foreign information operations. The office also liaises with representatives from Facebook, Google, Twitter, and Microsoft. "We showed initiative on this because at some point we understood is something happens, people will be looking at us anyway," said an advisor to the Estonian government on disinformation issues.[130] We recommend increasing funding for these offices in the Government Office and increasing staffing.

   Throughout the Baltic states, work on this issue will require a permanent staff, and Estonia is particularly well-placed to share best practices in strategic communications with Latvia and Lithuania. Estonia can act as a strategic partner with Latvia and Lithuania to explain methodologies behind the Public Opinion and National Defense survey,[131] the Integration Monitoring Survey,[132] and the mapping of seven key national attitudes that best describe the Estonian public's sentiment toward defense and security policies.[133]

[130] Interview with Estonian strategic communications expert, author interview, Tallinn, Estonia, January 16, 2019.
[131] Juhan Kivirähk, *Public Opinion and National Defence* (Tallinn, Estonia: Estonian Ministry of National Defence, 2018), http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/public_opinion_and_national_defence_2018_october.pdf.
[132] Kristjan Kaldur, Raivo Vetik, Laura Kirss, Kats Kivistik, Külliki Seppel, Kristina Kallas, Märt Masso, and Kristi Anniste, *Integration Monitoring of the Estonian Society 2017* (Tallinn, Estonia: Ministry of Culture, 2017), https://www.kul.ee/en/integration-monitoring-estonian-society-2017.
[133] Interview with Estonian strategic communications official, author interview, Tallinn, Estonia, January 16, 2019. Note: These seven key attitudes include (1) Readiness to participate in defense, (2) Participation in civil society organization related to defense and security, (3) Support for NATO membership, (4) Trust towards government institutions, (5) Support to EU membership, (6) Feeling of belonging to Estonian state / society, (7) Ethnic differentiation and association of cultural differences with conflict.

2. **Improve Quality of Programming and Funding for ETV+**
   Estonia and Latvia (and to a lesser extent Lithuania) should expand government funding for and involvement in programs to integrate their ethnic Russian and Russian-speaking minorities. Such an initiative would include the creation of alternative media content for ethnic Russians and the Russian-speaking minority. Previous research on this issue provides recommendations, including funding Russian-language programs and local media to work at a level that foreign broadcasters cannot achieve.[134] This report agrees with this conclusion.

Recommendations for Latvia

1. **Promote Russian-language investigative journalism**
   This report recommends the creation of digital media hubs, perhaps in cooperation with non-profit media funds, the EU or the US to support Russian-language journalists.[135] The creation of an independent TV channel for Latvia in the style of Estonia's ETV+ will remain a long-term goal in the future, however funding digital journalism represents a lower cost, and more immediate impact solution. Baltic Centre for Media Excellence represents the kind of organization that can better train and prepare digital journalists in the region. Government grants to young journalists, or the professionalization of journalism focused on the Russian-speaking part of the country would help improve the quality of reporting in the information space to give perspectives on issues that do not come directly from Kremlin-backed TV networks.

2. **Appropriate Funding for a Disinformation Education Campaign**
   Public education campaigns, ranging from statements by political leaders to funding of public-service announcements, should be widely practiced.[136] This campaign would include explanations via television, radio, film, and social media that information operations exist, and consumers should think critically when they engage with media from unverified sources.

3. **National Narrative Campaign**
   Latvia will require a national narrative public relations campaign. We recommend creating a position within the Latvian government to promote tourism, economic development, foreign investment so as to create a strategic "Brand Latvia." A national narrative campaign would be part of a larger advertising initiative to promote a positive image of the Latvian state. Given that one of Russia's main strategies is to sow discontent toward the Latvian state, this campaign would work to combat Russia's framing of Latvia's image. At the US state level, famous slogans include "I Love New York."

[134] Helmus, et al, "Russian Social Media Influence."
[135] Ibid.
[136] Daniel Fried and Alina Polyakova, Democratic Defense Against Disinformation (Washington: Atlantic Council, 2018), https://www.atlanticcouncil.org/images/publications/Democratic_Defense_Against_Disinformation_FINAL.pdf.

Within the Baltic states, the Estonian government's strategic communications message discipline pitching Estonia as a tech-hub stood out in our assessments. We recommend that Latvia adopt a similar strategy to put forward a positive image in contrast to that of Russian media. A national narrative would assist in diplomatic and government efforts to maintain a united message of what it means to be in Latvia in the 21st century.

Past slogans for Latvia that could be revisited, and updated for the future include:

Formal

- "Best enjoyed slowly" – developed by Adell Saatchi&Saatchi, a public relations firm to increase tourism to rural areas
- "Magnetic Latvia" – a brand developed to increase tourism, exports and promotion of foreign investment
- "Live Riga" – the city of Riga's economic development and tourism slogan
- "The Land that Sings" – a slogan that speaks to the "singing revolution" from 1987-1991 that led to the restoration of independence in the Baltic states

Informal

- "Green Latvia" – highlighting the fact Latvia has the fourth-highest forest cover among EU countries, and environmental progress in Latvia
- "Switzerland of the East" – highlighting the ease of doing business in Latvia

4. **Increase Military and Police Engagements with the Russian minority**
   This report recommends that Latvia adopt a social cohesiveness program similar to Estonia's Sinu Riigi Kaitse (Defence of Your Country) program. This type of program in the Latvian context would include career visits by the Latvian military or police to promote Latvian Estonian national identity among young ethnic Russians or Russian-speakers. Such a program would include visits to schools by Russian-speakers in Latvia's armed services, or creating a mentoring network among Russian-speaking professionals toward at-risk Russian-speaking youth in the Latgale region of Latvia.

Recommendations for Lithuania

1. **Formalize Elections Security Planning**
   Currently, election security planning operates on an ad hoc basis in the run-up to parliamentary elections. This report recommends a standing committee within the Lithuanian Bureau of Threat Management and Crisis that meets regularly devoted to issues of information operations and elections security. This committee would have responsibilities over pre-election simulations and exercises to build resiliency within the government in the event an information operation takes place. High-level security exercises, including table-top exercises, and crisis management crisis planning already

take place.[137] However, these exercises should be formalized according to a regular schedule and should include exercises on information operations and elections security.

2. **Improve Translation of Programming to Russian and Polish and Expand the Programming Reach of Lithuanian News into on Public Television**
   This report recommends expanding public programming to include conventional entertainment programming by cooperating with the Broadcasting Board of Governors (BBG) through Current Time TV, which targets audiences in Lithuania. Given that the concerns of the Polish minority toward the state of Lithuania are an emerging concern, and given the "soft" nature of Russian information operations via television, this kind of step on public television would help to provide different narratives than Kremlin-backed programming.

[137] Interview with Lithuanian government expert, author interview, Vilnius, Lithuania, January 18, 2019.

Appendix 4: Recommendation Criterion Analysis

Recommendation Criterion Analysis*

Overall Recommendations	Efficacy	Equity	Administrative Feasibility	Sustainability	Cost	Political Feasibility
Deepen Sharing of Intelligence, Best Practices, and Lessons Learned						
Resource Working Groups						
Invest in Monitoring and Explore Regulatory Approaches						
Craft and Promote Compelling, Unifying National Narratives						
Exercise and Stress-Test Contingency Plans						
Expand Investments in Election Cybersecurity						
Expand Integration Policies Targeting Russian Minority Populations						

Recommendation criterion analysis based on 45 inteviews and litature review.

Key

- Recommendation Strongly Supported by Interviews an Research Interviews
- Recommendation Moderately Supported
- Views Mixed on this Metric
- Recommendation will find moderate challenges
- Recommendation will find challenges

Country-Specific Recommendation Criterion Analysis*

Country-Specific Recommendations	Efficacy	Equity	Administrative Feasibility	Sustainability	Cost	Political Feasibility
Estonia						
Improve Quality of Programming and Funding for ETV+						
Increase Funding and Staffing for Strategic Communications						
Latvia						
Promote citizen fact-checking and investigative journalism						
National Narrative Campaign						
Appropriate Funding for a Disinformation Education Campaign						
Increase Military and Police Enagements with Russian minority						
Lithuania						
Improve Translation of Lithuanian News into Russian on Public Television						
Formalize Elections Security Planning						

Country-specific analysis based on 45 inteviews and litature review.

Key

- Recommendation Strongly Supported by Interviews an Research Interviews
- Recommendation Moderately Supported
- Views Mixed on this Metric
- Recommendation will find moderate challenges
- Recommendation will find challenges

Appendix 5: Works Cited

"Action Plan against Disinformation." *European Commission*, December 5, 2018. https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

Alliksaar, Kalsa, and Matthew Luzmoore. "'Only Estonians Here': Outrage After Election Poster Campaign Singles Out Russian Minority." *Radio Free Europe/Radio Liberty*, January 10, 2019. https://www.rferl.org/a/estonia-election-posters-russian-minority-outrage/29702111.html.

"Ambiguous Threats and External Influences in the Baltic States: Phase 2: Assessing the Threat." *Asymmetric Operations Working Group*, November 2015. https://www.stratcomcoe.org/ambiguous-threats-and-external-influences-baltic-states.

Anniste, Kristi, Kristjan Kaldur, Kristina Kallas, Laura Kirss, Kats Kivistik, Märt Masso, Külliki Seppel, and Raivo Vetik. *Integration Monitoring of the Estonian Society 2017.* (Tallinn, Estonia: Ministry of Culture, 2017). https://www.kul.ee/en/integration-monitoring-estonian-society-2017.

Antson, Agaate, and Sander Punamae. "Estonia 200 provocative posters." *Postimees*, January 8, 2019. https://news.postimees.ee/6494099/estonia-200-provocative-posters.

Bajarunas, Eitvydas. "Lessons from the Baltic States: strengthening EU resilience against Russian hybrid warfare." In *Hybrid and Transnational Threats: Discussion Paper*, edited by Jamie Shea. Brussels: Friends of Europe, 2018. https://www.friendsofeurope.org/sites/default/files/2018-12/FoE_SEC_PUB_Hybrid_DP_WEB.pdf.

Beauchamp-Mustafaga, Nathan, Scott Boston, Michael Johnson, and Yvonne K. Crane. *Assessing the Conventional Force Imbalance in Europe: Implications for Countering Russian Local Superiority*. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2402.html.

Bega, Andriy, Elizabeth Bodine-Baron, Todd C. Helmus, Madeline Magnuson, William Marcellino, Joshua Mendelsohn, Andrew Radin, and Zev Winkelman. *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf.

Bentzen, Naja. "Online disinformation and the EU's response." *European Parliamentary Research Service*, 2019. http://www.europarl.europa.eu/RegData/etudes/ATAG/2018/620230/EPRS_ATA(2018)620230_EN.pdf.

Beyrle, John R. "The Long Good-Bye: The Withdrawal of Russian Military Forces from the Baltic States." *Institute for the Study of Diplomacy, Georgetown University*, 1996.

Bienvenue, Emily, Zac Rogers, and Sian Troath. "Cognitive Warfare: The Fight We've Got," *Cove*, September 19, 2018. https://www.cove.org.au/adaptation/article-cognitive-warfare-the-fight-weve-got/.

Boston, Scott and Dara Massicot. *The Russian Way of Warfare: A Primer*. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/perspectives/PE231.html.

Brattberg, Erik, and Tim Maurer. *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*. Washington: Carnegie Endowment for International Peace, May 2018. https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf.

Calamur, Krishnadev. "Putin Says 'Patriotic Hackers' May Have Targeted U.S. Election." *The Atlantic*, June 1, 2017. https://www.theatlantic.com/news/archive/2017/06/putin-russia-us-election/528825/.

Conley, Heather, Donatienne Ruy, Ruslan Stefanov, and Martin Vladimirov. *The Kremlin Playbook 2*. Washington: Center for Strategic and International Studies, 2019. https://www.csis.org/features/kremlin-playbook-2.

Digital Forensic Research Lab. "#ElectionWatch: Graphic Preference from Russian Media in Latvia." *Atlantic Council*, September 24, 2018. https://medium.com/dfrlab/electionwatch-graphic-preference-from-russian-media-in-latvia-44853a34e9c4.

Ee, Shaun and Laura Galante. *Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents*. (Washington: The Atlantic Council, September 2018). https://www.atlanticcouncil.org/images/publications/Defining_Russian_Election_Interference_web.pdf.

Ekmanis, Indra, "The Non-Citizen Non-Question: Latvia Struggles to Leave Soviet Legacy Behind," *Foreign Policy Research Institute*, October 18, 2017. https://www.fpri.org/article/2017/10/non-citizen-non-question-latvia-struggles-leave-soviet-legacy-behind/.

Estonian Foreign Intelligence Service. "International Security and Estonia 2019." 2019. https://www.valisluureamet.ee/pdf/raport-2019-ENG-web.pdf.

"Eurobarometer Survey 90 of the European Parliament: A Public Opinion Monitoring Study." *European Parliament*, 2018. http://www.europarl.europa.eu/at-your-service/files/be-heard/eurobarometer/2018/parlemeter-2018/report/en-parlemeter-2018.pdf.

European Union Agency for Network and Information Security (ENISA). "National Cyber Security Strategies." 2019, accessed March 14, 2019. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

"FACT SHEET: The United States and Estonia, Latvia, and Lithuania – NATO Allies and Global Partners." *U.S. Embassy in Latvia,* August 23, 2016. https://lv.usembassy.gov/u-s-baltic-summit-readout-2/?_ga=2.34192161.181103584.1554039661-239102275.1554039661.

Federal Ministry of the Interior. "German National Cyber Security Strategy." 2011. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-for-germany/view.

Fried, Daniel and Alina Polyakova. *Democratic Defense Against Disinformation*. Washington: Atlantic Council, 2018. https://www.atlanticcouncil.org/images/publications/Democratic_Defense_Against_Disinformation_FINAL.pdf.

Friedman, Uri "Here's What Foreign Interference Will Look Like in 2020," *The Atlantic*, August 9, 2019. https://www.theatlantic.com/politics/archive/2019/08/foreign-election-interference-united-states/595741/.

Gelzis, Gederts. "Latvia says Russia targeted its foreign and defense bodies with cyber attacks." *Reuters*, October 8, 2018. https://www.reuters.com/article/us-latvia-russia-cyber/latvia-says-russia-targeted-its-foreign-and-defense-bodies-with-cyber-attacks-idUSKCN1MI1SB.

Gillett, Francesca. "Electoral Commission launches probe into Russian meddling in Brexit vote using Twitter and Facebook." *The Evening Standard*, November 2, 2017. https://www.standard.co.uk/news/politics/election-watchdog-launches-probe-into-russian-meddling-in-brexit-vote-a3674251.html.

Goel, Arya; Martin, Diego and Shapiro, Jacob, "Managing and Mitigating Foreign Election Interference," *Lawfare,* July 21, 2019. https://www.lawfareblog.com/managing-and-mitigating-foreign-election-interference

Grigas, Agnia. *Beyond Crimea: The New Russian Empire*. New Haven: Yale University Press, 2016.

Grigas, Agnia. "Compatriot Games: Russian-Speaking Minorities in the Baltic States." *World Politics Review*, October 11, 2014. https://www.worldpoliticsreview.com/articles/14240/compatriot-games-russian-speaking-minorities-in-the-baltic-states.

Hartmann, Margaret. "Facebook Haunted by Its Handling of 2016 Election Meddling." *New York Magazine*, March 20, 2018. http://nymag.com/intelligencer/2018/03/facebook-haunted-by-its-handling-of-2016-election-meddling.html.

Ilves, Toomas Henrik, "Forward: Toomas Henrik Ilves, President of the Estonian Republic." In *E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015)*, edited by Mihkel Solvak and Krisjan Vassil. Tartu: Johann Skytte Institute of Political Science, University of Tartu, 2016.

Kallas, Kristina. "Claiming the diaspora: Russia's compatriot policy and its reception by Estonian-Russian population." *Journal on Ethnopolitics and Minority Issues in Europe*, Vol. 15, No. 3, (2016). https://www.ecmi.de/fileadmin/downloads/publications/JEMIE/2016/Kallas.pdf.

Koorits, Vahur. "Eestlased ja venelased saatis trammipeatuse eraldi nurkadesse Eesti 200." *Delfi*, January 7, 2019. https://www.delfi.ee/news/rk2019/uudised/eestlased-ja-venelased-saatis-trammipeatuse-eraldi-nurkadesse-eesti-200?id=84956185.

Kivirähk, Juhan. *Public Opinion and National Defence*. Tallinn, Estonia: Estonian Ministry of National Defence, 2018. http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/public_opinion_and_national_defence_2018_october.pdf.

"The Kremlin election compass." *Propastop*, February 19, 2019. https://www.propastop.org/eng/2019/02/19/the-kremlin-election-compass/.

Kroet, Cynthia. "Russia spread fake news during Dutch election: report." *Politico*, April 4, 2017. https://www.politico.eu/article/russia-spread-fake-news-during-dutch-election-report-putin/.

Latvian Central Statistical Database, 2018, accessed March 31, 2019, https://data.csb.gov.lv/pxweb/lv/iedz/iedz__iedzrakst/IRG080.px/?rxid=cd00d9dc-a4e4-4b85-a975-e8b416dee23e.

Maza, Cristina. "Vladimir Putin's Adviser Tells Americans: 'Russia Interferes in Your Brains, We Change Your Conscience.'" *Newsweek*, February 12, 2019. https://www.newsweek.com/russia-president-vladimir-putin-election-americans-1327793.

McGeehan, Timothy P., "Countering Russian Disinformation," *Parameters*, 48(1), (U.S. Army War College, 2018). https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/8_McGeehan_CounteringRussianDisinformation.pdf.

Menn, Joseph and Dustin Volz. “Twitter suspends Russia-linked account, but U.S. senator says response inadequate.” *Reuters*, September 28, 2017. https://www.reuters.com/article/us-usa-trump-russia-twitter-idUSKCN1C331G.

Mook, Robbie, Matt Rhoades, et al. *Cybersecurity Campaign Playbook: European Edition*. Cambridge, MA: Belfer Center for Science and International Affairs, 2018. https://www.belfercenter.org/sites/default/files/files/publication/EuropeanCampaignPlaybook.pdf.

“National Cyber Strategy of the United States of America.” The White House, September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Office of the Director of National Intelligence. “Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections.” January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Petsinis, Vassilis. “As long as it lasts: Latvia’s new coalition government.” *openDemocracy*, January 26, 2019. https://www.opendemocracy.net/en/can-europe-make-it/as-long-as-it-lasts-latvia-s-new-coalition-government/.

“A Political Scandal in Estonia and Russian Influence in the Baltics.” *Stratfor*, December 27, 2010. https://worldview.stratfor.com/article/political-scandal-estonia-and-russian-influence-baltics.

Popescu, Nicu. “Russian cyber sins and storms.” *European Council on Foreign Relations*, October 10, 2018. https://www.ecfr.eu/article/commentary_russian_cyber_sins_and_storms.

Premier Ministre. “French National Digital Security Strategy.” 2015. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/information-systems-defence-and-security-frances-strategy.

Rettman, Andrew. “Exposed: How Russia offered to fund Italy's Salvini.” *EuroOberver*, February 25, 2019. https://euobserver.com/foreign/144253.

Rosenbach, Eric. “America, Democracy and Cyber Risk: Time to Act.” Testimony to the United States Senate Committee on Homeland Security and Governmental Affairs, April 24, 2018. https://www.hsgac.senate.gov/imo/media/doc/Testimony-Rosenbach-2018-04-24.pdf.

Schmidt, Andreas. “The Estonian Cyberattacks.” In *The fierce domain – conflicts in cyberspace 1986-2012,* edited by Jason Healey. Washington: Atlantic Council, 2013. https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks.

Senate Intelligence Committee. “Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations.” May 8, 2018.

https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

Shane, Scott. “These Are the Ads Russia Bought on Facebook in 2016.” *The New York Times*, November 1, 2017. https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html.

Siboni, Gabi. “The First Cognitive War.” In *Strategic Survey for Israel 2016-2017*, edited by Anat Kurz and Shlomo Brom. Tel Aviv: Institute for National Security Studies, 2016. https://www.inss.org.il/publication/first-cognitive-war/.

Statistics Estonia. “Population by Sex, Ethnic Nationality and County.” January 1, 2018, accessed March 31, 2019. https://www.stat.ee/population-indicators-and-composition.

Surkov, Vladislav. “Долгое государство Путина.” Независимая газета, February 11, 2019. http://www.ng.ru/ideas/2019-02-11/5_7503_surkov.html.

Turovsky, Daniil. “‘It’s our time to serve the Motherland’ How Russia’s war in Georgia sparked Moscow’s modern-day recruitment of criminal hackers.” *Meduza.io*, August 7, 2018. https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland.

Underwood, Kimberly. “Cognitive Warfare Will Be Deciding Factor in Battle.” *SIGNAL Magazine, August 15, 2017*. https://www.afcea.org/content/cognitive-warfare-will-be-deciding-factor-battle.

Vilmer, Jean-Baptiste Jeangene. *Successfully Countering Russian Electoral Interference: 15 Lessons Learned from the Macron Leaks*. Washington: Center for Strategic and International Studies, June 2018). https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180621_Vilmer_Countering_russiam_electoral_influence.pdf?qFOz5qjpEuTzu5cvUa.UgOj0Dg3FklQP.

Wafford, Benjamin. “The hacking threat to the midterms is huge. And technology won’t protect us.” *Vox*, October 25, 2018. https://www.vox.com/2018/10/25/18001684/2018-midterms-hacked-russia-election-security-voting.

Wilson, Andrew. “Four Types of Russian Propaganda.” *Aspen Review*, Issue 4 (2015). https://www.aspenreview.com/article/2017/four-types-of-russian-propaganda/.

Winnerstig, Mike, ed. *Tools of Destabilization: Russian Soft Power and Non-military Influence in the Baltic States*. Stockholm: FOI, 2014. http://appc.lv/wp-content/uploads/2014/12/FOI_Non_military.pdf.

Wintour, Patrick. “Russian bid to influence Brexit vote detailed in new US Senate report.” *The Guardian*, January 10, 2018. https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report.

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org