WILL AND CAPABILITY: WESTERN GOVERNMENTS' RESPONSE TO RUSSIAN DISINFORMATION SINCE 2013

Brian McDowell

A DISSERTATION

in

Political Science

Presented to the Faculties of the University of Pennsylvania

in

Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

2022

Supervisor of Dissertation

Matthew Levendusky

Professor, Political Science

Graduate Group Chairperson

Rudra Sil, Professor, Political Science

Dissertation Committee

Michael C. Horowitz, Richard Perry Professor, Political Science
Marc Meredith, Associate Professor, Political Science
Alex Weisiger, Associate Professor, Political Science

WILL AND CAPABILITY: WESTERN GOVERNMENTS' RESPONSE TO RUSSIAN DISINFORMATION SINCE 2013

For Max and Grant.
And for Dad.

ACKNOWLEDGMENT

Throughout the writing of this dissertation, I have received a great deal of support and assistance.

I would first like to thank my Committee Chair, Professor Matthew Levendusky, whose expertise and feedback at every step was invaluable in formulating my questions, methodology, and ideas. I would also like to acknowledge the feedback from all other members of my committee; your collective insight pushed me to sharpen my thinking and brought my work to a higher level.

I would like to acknowledge my colleagues in Penn's Political Science Department and in the Army's Advanced Strategic Planning and Policy Program (ASP3). The last three years have been challenging. You have provided motivation, collaboration, and friendship to stay on track and successfully complete my dissertation.

I could not have finished this dissertation without the support of my friends—especially the Golden Cohort, the Cush Brothers' Retreat, and the National Insecurity Forum, who all provided stimulating discussions as well as happy distractions to rest my mind outside of my research.

Finally, nobody has been more important to me in the pursuit of this project than the members of my family. I would like to thank my brother and sister-in-law for allowing me several valuable writing trips. Most importantly, I wish to thank my loving and supportive wife, Tracy, and my boys, Max and Grant. Writing a dissertation is ultimately an individual effort, but it requires a team; you gave me cover by taking up the slack every time I disappeared to focus. That was more often than I had any right to ask—so thank you. I love you!

ABSTRACT

WILL AND CAPABILITY: WESTERN GOVERNMENTS' RESPONSE TO RUSSIAN DISINFORMATION SINCE 2013

Brian McDowell

Matthew Levendusky

In 2013, the Kremlin resourced and launched a multiyear global operation to subvert democracy. The operation's main weapon was intentionally harmful information—disinformation—spread through networks of paid trolls, bot networks, and users around the world. The information was aimed at sowing division within democracies and between democracies, particularly in NATO and the European Union. Some governments chose stronger responses than others. What explains the variation in government responses? I argue that each democracy's combination of will and capability determined its response and that states with similar endowments of will and capability chose similar policies. I conduct an in depth cross-national of thirteen Western democracies supported by two case studies of specific states: Finland and the United States. My findings show that Kremlin disinformation has repeatedly adapted to changing contexts over the last century, is likely to continue adapting, and that Kremlin tactics having shown effectiveness, have spread to more state governments and even domestic actors. Future attacks will likely follow similar themes and patterns, so the lessons learned in this dissertation can help inform future responses.

TABLE OF CONTENTS

LIST OF TABLES

PREFACE

As Senator Cardin noted ahead of transmitting a 2018 minority staff report to the Committee on Foreign Relations:

> It is important to draw a distinction between Mr. Putin's corrupt regime and the people of Russia. Many Russian citizens strive for a transparent, accountable government that operates under the democratic rule of law, and we hold hope for better relations in the future with a Russian government that reflects these demands. In the meantime, the United States must work with our allies to build defenses against Mr. Putin's asymmetric arsenal and strengthen international norms and values to deter such behavior by Russia or any other country.[1]

Throughout this dissertation, any reference to "Russia" or "Russian" refers not to the people of Russia, but to the country's political leadership. These terms are used synonymously and with "the Kremlin," mixed to avoid repetitiveness, and meant to indicate the regime led by President Vladimir Putin.

1. See "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for United States National Security", 2018, p. vi.

CHAPTER 1
INTRODUCTION

"The most amazing information warfare blitzkrieg we have ever seen in the history of information warfare"
-General Philip Breedlove, Supreme Allied Commander Europe. September 2014.[2]

The Issue of Russian Disinformation

Much of the United States became familiar with Russian disinformation during and after the 2016 Presidential election. Contrary to popular sentiment at the time, the Kremlin attack on a United States election was not a one-off attack against American democracy. Rather, the attack was part of an ongoing and accelerating global operation aimed at subverting the democratic world order.

Students of disinformation have defined several concepts that aid in discussing the operation. For example, misinformation is simply incorrect information. Incorrect information matters in a democracy because, as Kuklinski writes:

> people often are not *un*informed about policy… but *mis*informed. People hold inaccurate factual beliefs and do so confidently. The problem, then, at least with respect to attitudes about public policy, is not that people simply lack information, but that they firmly hold the wrong information—and use it to form preferences. Not only does this misinformation function as a barrier to factually educating citizens, it can lead to collective preferences that differ significantly from those that would exist if people were adequately informed.[3]

By contrast, disinformation is "information that is false and deliberately created to harm a person, social group, organization or country."[4] So disinformation can be created by an attacker to cause harm, spread by other malicious actors, or spread by neutral and unwitting users as misinformation. Additionally, disinformation and misinformation can

2. Quoted in Pomerantsev, 2014.
3. Kuklinski, et al., 2000, p. 792.
4. Wardle, et al., 2017, p. 20.

be amplified through inauthentic accounts, bots, and impostors online using the anonymity afforded by many platforms. As Former President Obama recently detailed in a speech, the amplification and spread of disinformation and misinformation using digital tools presents has grown into a challenge to democracy itself.[5]

The Kremlin adopted a strategy that intentionally combined disinformation, digital media, and inauthentic accounts in 2013, which became a turning point for subverting democracy through disinformation. In the months immediately preceding Russia's February 2014 illegal annexation of Crimea and invasion of Eastern Ukraine, the Kremlin launched an operation that ushered in a new era in information operations.[6] Moscow had by then been experimenting for several years in applying digital propaganda as part of a suite of capabilities aimed at degrading adversaries in ways historically associated with military invasion.[7] Russia had applied disinformation coordinated with cyberattacks, military invasion, diplomatic pressure, economic coercion, and other elements of state power to pursue a series of aggressive actions in Ukraine, Estonia, Georgia, and others. But while initially focusing on Ukraine in 2013, the Kremlin swiftly escalated its information operations against a host of nations globally, not just those that neighbored Russia. This was the beginning of a sustained global assault on the United States-led democratic world order.

5. Dwoskin and Scott, 2022.
6. Vandiver, 2014.
7. Pynnöniemi, 2019, p. 159. "In traditional understanding, an armed conflict (war) means the physical destruction of the enemy. At the same time, an attack can be regarded as successful when it leads to the "self-disorganization" and "self-disorientation" of the adversary, and the subsequent capture of the enemy's resource base and its usage to the benefit of the attacker."

The operation which began with a goal of creating confusion to provide cover for its imminent annexation of Crimea later morphed into the sprawling international effort that so brazenly attacked the American election. [8] The operation also included significant attacks on many other democracies including Brexit in the United Kingdom, election interference across Europe, fomenting multiple border crises in Norway, Finland, and Poland, enflaming separatist movements in Spain and the United States, and spreading emotionally charged disinformation about child custody cases in multiple countries.[9]

Ben Nimmo and his Graphika coauthors (2020) dubbed the operation "Secondary Infektion." This name is a nod to a successful 1980s Soviet operation, Operation Infektion, which blamed the United States for developing AIDS as a bioweapon.[10] The former Naval cryptologist and intelligence expert Malcolm Nance called the operation "Global Grizzly."[11] Whatever name one applies to the operation, it was a remarkably ambitious and sweeping effort.

The Kremlin's main weapon in this operation was the now infamous Internet Research Agency (IRA) troll farm in St. Petersburg.[12] The hundreds of trolls operated thousands of accounts to seed division through false narratives, mostly on social media. These narratives were amplified by an army of bots to accomplish several different Russian aims. Lucas et al., 2021 provide a good list of Moscow's motivations:

> The Russian regime's foremost interest is its own hold on power. All policy, internal and external, stems from this overriding goal. The Kremlin sees the West, the European Union (.), and NATO as threats to this stability, and as potential instigators of "color revolutions" that will exploit Russia's ethnic,

8. Vandiver, 2014.
9. Nance and Reiner, 2018.
10. Nimmo et al., 2020.
11. Nance and Reiner, 2018.
12. Nimmo et al., 2020.

> religious, political, and other fissures. The long-term goal is, therefore, a polycentric or multipolar world in which multilateral, rules-based organizations are unable to dictate terms to Russia. Instead, the Kremlin aims to be the dominant power in Eurasia, using Russia's size to exert strong influence over its neighbors and over small countries, and to bargain with big countries on an equal basis.[13]

Disinformation was not simply a supporting effort in this campaign, it was a weapon. To accomplish its operational objectives, the Kremlin pushed thousands of false, manipulative, incendiary, and sometimes plainly ridiculous stories. Ben Nimmo's team analyzed 2,500 articles, for example, to map the operation's themes. By far the top three narratives focused on portraying Ukraine as an unreliable failed state (830 articles), NATO and the West as aggressors (536 articles), and the European Union as weak and divided (508 articles).[14] The attacks continued at a dizzying pace and targeted all pro-democratic states with tailored messaging designed to exacerbate existing divisions—both within and between— democratic states.

Each of the targeted countries responded in different ways. Some acted to prevent widespread acceptance of false narratives within their populations and other states did not. The United Kingdom, for example, developed rapid response mechanisms that monitored false Kremlin narratives and ensured algorithms prioritized availability of official United Kingdom Government sources.[15] By contrast, the Polish Government chose to target internal political dissent with populist disinformation of its own, ignoring the Russian threat and suffering major declines in scores for democratic health.[16] This

13. Lucas et al., 2021
14. Nimmo et al., 2020
15. See Levush, 2019.
16. See Gregor and Mlejnková, 2021 and Kosc, 2020.

dissertation aims to explain the varied responses by a wide range of democratic governments that were targeted with Russian disinformation campaigns.

I argue that democratic state responses to disinformation are the result of each state's combination of will and capability at the time of an attack. In my framework, the United Kingdom is a high will high capability state. I expect high will high capability states to be leaders protecting democracy domestically and internationally. And by contrast again, Poland is a low will low capability state. I expect low will low capability democracies to do little or nothing responding to disinformation attacks while the intended corrosive effects manifest in weakened institutions. The states with high will and low capability or low will and high capability should make similar policy choices to states similarly endowed, and states can move between groups over time since the two variables are not fixed. While capabilities can ebb and flow, they generally take longer to develop than the more volatile will. When Russian aggression operates below the threshold of public reaction, will recedes. But when a democratic state perceives it is under subversive attack, will to resist can rapidly increase. All of this is outlined in Chapters 2 and 3.

Before analyzing democratic responses, however, it is essential to first define the nature and scope of Russian disinformation campaigns. Of course, such efforts did not begin de novo in 2013 when Moscow invaded Crimea. Instead, these efforts drew on decades of Soviet disinformation tactics and doctrine, adapted and honed during the first decade of President Vladimir Putin's first decade in power, and only later unleashed on an unevenly prepared democratic West.

Russian disinformation has roots in Soviet doctrine. As far back as Lenin, Soviet

thinking about disinformation has posited that it should always be tied to the physical world.[17] Information is not an abstraction, but itself a tool for contestation. It should be used internally to organize and externally to disorganize. So, information, spread as propaganda should always be aimed at a concrete goal and it must always adapt to changing contexts.[18] Context includes changes in media landscape, relations with Russia, and internal cultures of other states. Early in his presidency, Vladimir Putin began a campaign to prioritize regaining Soviet-like information dominance— domestically at first and then internationally. And as Soviet thinkers like Lenin outlined, the Russian approach adapted to a changed context.

Throughout decades of Soviet propaganda efforts, influencing Western audiences required elaborate efforts to create forgeries, generate misleading print newspaper and journal articles, and cultivate reliable messengers who could credibly promote Kremlin narratives.[19] These efforts were mostly inefficient. Western broadcast media was concentrated and controlled, so gaining amplification required a message to make it through many layers of filters before any opportunity to reach wide audiences.

By 2000, the media context had changed. When President Putin took power, he immediately prioritized pushing back on Western influence; within the first few years of his presidency, he prioritized creation of powerful media organizations oriented on

17. See Pynnöniemi, 2019, p. 157. "The underlying idea expressed in one form or another in this debate is derived from Lenin, who asserted that propaganda should be a matter of action rather than words. In the Soviet propaganda campaigns that followed, this idea was interpreted to mean that all agitation should be tied to some concrete goal."
18. See Pynnöniemi, 2019, p. 163. "Two issues should be highlighted in this connection. First, while Active Measures have a systemic character (and certain patterns can be observed in themes and narratives), Lenin's dictum about working with material is still important. This means that the context (historical relations with Russia, criminal environment, media space, etc.) shapes the ways in which Active Measures are used."
19. Rid, 2020.

competing globally in a media environment that now included influential cable news networks. Russia's answer was the creation of RT, Sputnik, and other outlets to get Russian narratives included directly into Western media environments in ways inconceivable in Soviet times. [20] As social media grew through the late 2000s and early 2010s, capabilities for tailored messaging and reach to individual users offered even greater opportunities for meddling. The Kremlin created an increased ability to reach users directly in formats that looked, sounded, and felt credible to Western audiences.

Not only did Putin adapt to a changing media environment, but he also adapted the messaging. Russian disinformation goals are different than their Soviet predecessors. While the Soviet Union and the United States competed in a bipolar order, each working to supplant the other, competition between Russia and the United States is different. After the Cold War, the United States emerged as the hegemon in a unipolar order. It benefits most from structuring and protecting the order. Russia, unable to compete directly, has used disinformation as part of a strategy to subvert that order.[21] This is a key difference from Soviet times; Russia does not seek to replace United States order with anything, instead the Kremlin is operating in a zero-sum competition assessing that it wins just by making democracies less attractive.

Garry Kasparov summed up the challenge succinctly: "The point of modern propaganda isn't only to misinform or push an agenda. It is to exhaust your critical

---

20. See "Fog of falsehood: Russian strategy of deception and the conflict in Ukraine", 2016, p. 48. "The two most emblematic actors are RT and Sputnik, in addition to a wide network of information websites and groups on social media networks. The Soviet Union was never able to massively implant its own messages and narratives into mainstream Western media… Contrary to the Soviet times, however, now Moscow can easily and steadily reach Western consumers, and thus deliver its propaganda and disinformation messages directly."
21. Radin et al., 2020, p. 3

thinking, to annihilate truth."[22] The changes in media landscape and regime goals make modern propaganda a decidedly new twist on an old problem. Once truth is eliminated, debate becomes impossible and those with the loudest megaphones can rule by dictate. As Snyder wrote, post-truth is pre-fascism: "When we give up on truth, we concede power to those with the wealth and charisma to create spectacle in its place. Without agreement about some basic facts, citizens cannot form the civil society that would allow them to defend themselves."[23] Seeing an opportunity to use disinformation to subvert the West,[24] Russia pressed its advantage by pouring money, people, and its considerable cultural expertise into a sprawling campaign against democracy everywhere.[25] Western democracies varied in their responses to this subversive operation.

Core Argument

My claim in this dissertation is that while there are myriad factors at play in an anarchic international political environment, it is each state's combination of will and capability that broadly explain differences in policy choices. This is true both for the Kremlin's choice to fund disinformation operations as an attack against democracy, as well as for the democratic states' response to those operations. There exists a wide spectrum of policy options available to combat disinformation. Some of the most common options include inaction, downplaying or ignoring the threat, bolstering

22. Quoted in Bjola and Papadakis, 2020, p. 638
23. Snyder, 2021.
24. See Pomerantsev and Weiss, 2014, p. 20. "Putin is onto something big... He has discovered a significant weapon with which to beat the West and divide its potential allies around the world... In short, Vladimir Putin knows what he's doing."
25. See Radin et al., 2020, p. 3. "The Kremlin's financial and human resources give it a unique ability to mimic and influence legitimate social groups in ways that are often not discovered until long after they are perpetrated, if they are recognized at all."

democratic norms domestically, building coalitions to isolate Russia internationally, employing sanctions, updating legal frameworks to slow amplification, manipulating algorithms, enabling civilian organizations, creating new counter-disinformation organizations, clarifying false narratives, educating publics, or even deploying Russian disinformation domestically. If each state's choices result from its relative ability to act (it's capability) and desire to act (it's will), then I expect there should be trends among states grouped by comparable will and capability.

Chapter 2 makes this argument in detail. In brief, will is a state's commitment to resisting disinformation. Russia employs disinformation to challenge the existing international system in ways that typically involved physical fighting to accomplish. Although in some cases Russia has in recent years invaded and occupied neighboring states, it has not invaded a major western democracy seeking to destroy its national capabilities or political system. Attacking a NATO member would result in armed conflict with a unified military alliance of thirty nations. This direct confrontation would be suicidal. Russia therefore adapts its strategy, seeking instead asymmetric weapons like disinformation to weaken democracies from within. In different cases, Russia uses disinformation to impose its will on adversary states through narratives or reflexive control, creates space for maneuver by confusing adversary decision making, undermines faith in truth itself through whataboutism, and undermines morale through fear. All these effects are particularly dangerous to democracy which fundamentally depends on reliable information to enable effective collective judgements from which democratic regimes derive legitimacy. Undermining information, especially at critical points like elections,

can change a result, affect policy, undermine faith in institutions, or force a state to turn inward away from Russian actions abroad. All these attack democracy by subverting will.

In this dissertation, the concept of state will is the decision to counter effects of Russian disinformation attacks and the ability to sustain efforts to counter disinformation over time. Will springs from factors such as perceived intensity and persistence of threat, unity and social cohesion, trust in government, structure of political system, elite behavior, and commitment to democratic norms. In the short term, a state's will can be considered fixed; creating will in an open society requires trust, education, coordination, and competence. All take time to develop. Shocking attacks like Pearl Harbor or 9/11 can generate will quickly within democratic systems, but disinformation is designed as a slow burn. The Kremlin's intended effect is not disrupting will in the short term, but through long term systemic subversion. Dew describes the Kremlin's goal as incrementally "weakening the internal cohesion of societies and strengthening the perception of the dysfunction of the Western democratic and economic system"[26] to give Russia freedom of action. Will determines how intensely a state will or will not respond to disinformation.

The other main variable, capability, determines what options are available from which to choose. A state's capabilities responding to Russian disinformation results from different component elements of its power, including its aggregate national power, cyber capabilities, geography, leadership and governance, economic power, industrial and technological capacity, military power, ideology, diplomacy, national character and

26. Dew, 2019, p. 156.

morale, and foreign support. Some states are closer to Russia than others. Most Western democracies are richer than Russia. Some are more capably governed and ideologically committed to democracy than others. The menu of options available to each state derives from its capabilities. More capable states will naturally have more options from which to choose. But not all capability translates into effective response to disinformation operations. Raw military power or nuclear capability, for example, are not practically useful in fighting disinformation.

Of course, while aggregate capabilities are important, they do not tell the complete story. To dig deeper, I also considered states' disinformation-specific capabilities. A state's overall capabilities and its capabilities in controlling information environments will determine its range of available responses.

Sorting states by high and low will and capability allows some predictions for each group. Expectations appear in the quad above and are detailed in Chapter 2. High will, high capability democratic states should be the leaders pushing back against disinformation employing capabilities not only within their own societies, but also working to bolster and protect democratic norms internationally. High will, low capability states should be innovative protectors of domestic institutions and norms, building resilient societies and maximizing participation in international efforts as a defense against Russian aggression. I expect low will, high capability states to experience democratic backsliding since their governments will respond to the threat weakly or not at all. As democracy erodes, the capabilities resident in these states will eventually even be turned towards targeting disinformation at domestic populations accelerating divisions

already inflamed by Kremlin efforts. Finally, low will, low capability states are likely to do nothing at the state level. This creates a vacuum which will be filled by uncoordinated responses by non-state entities. These states will also experience backsliding as disinformation corrodes their democracies.

Methods and Case Selection

To explore my framework around will and capability, this dissertation employs a mix of methods: grounded theory research, case studies, and practitioner research. Grounded theory involves researching actions taken by a select group of democracies and coding their responses at the state level to see what patterns emerge. Case studies then explore specific states in greater depth and in historical context. And practitioner research rounds out the study by considering national security doctrines, and expert testimony, and document analysis. These approaches complement each other to provide a comprehensive understanding of how Western democracies responded to the Russian operation since 2013. The overall structure of the project includes three main sections: a cross-national comparison of actions taken to address Russian disinformation, a case study on Finland's actions, and a case study on the United States' actions.

First, I conducted a cross-national survey focusing on how thirteen countries each responded to Russian disinformation campaigns, compared to how my model predicted they would respond. Each is a democracy, has been attacked as part of Russia's post-2013 disinformation operation, and is either a NATO member or enjoys privileged relationships with NATO (i.e., they are Extended Opportunity Partners, or EOPs). Hybrid and new threats, including information warfare, are part of the reasoning for granting a

state Enhanced Opportunity Partner status so including them rounds out the list of states most relevant to investigating democratic response to Russian disinformation. Selection of these states is covered in greater detail in Chapter 3.

As a complement to this broad cross-national survey, I also researched case studies to explore state responses in greater depth. This dissertation includes two case studies: Finland and the United States of America. While the cross-national survey allows me to examine the key elements of a wide variety of nations, case studies are an opportunity for me to delve much more deeply into the mechanisms by considering both sides of a disinformation attack: the attacker and the attacked. Case studies allow room to explore the different ways Russia uses similar themes and tactics modified for country-specific targets and goals. Although Russian themes repeat, attacks are highly designed to exploit the differences in the Finnish and American societies. Further, case studies allow for more specific discussion of varying capabilities and limitations that impact domestic decisions within two very different democracies. Finally, case studies better describe how outcomes conform— or not— to expectations of my theory. These factors drove my focus on two states that are sufficiently different from each other that their study enhances understanding of variance within democracies writ large.

Finland, as a full democracy that borders Russia, has for decades been a target of Kremlin subversion. It and the United States are in opposite quadrants within my two-by-two framework of will and capability. Finland is high will and low capability. It is a small NATO Enhanced Opportunity Partner. Russia has long sought to destabilize the country internally, fomenting divisions between Finland and Europe, and preventing Finland from

full membership in NATO. Finland has been a model, however, for responding comprehensively to the threat from Russian disinformation. It is a good case study to understand the full array of options available for responding to disinformation.

On the other hand, the United States is a low will high capability state. When attacked during Russia's operation, the United States struggled. It responded sub optimally to disinformation— both from Russia and from within. The threat of domestic disinformation largely follows similar tactics of Russian disinformation but is potentially even more corrosive to democracy than external attack. I will now briefly introduce some key definitions used in this project.

Case Summaries

Cross-national Survey

Looking across my 13 nations, while there was a general correspondence between predictions and reality, there was some important, and theoretically informative, variation as well. States in the high will and high capability grouping include Canada, France, Germany, and the United Kingdom. My theory predicted that these states should lead democratic pushback against Russian disinformation, using a mix of offense to punish Russia and defense to protect democratic norms.

Except for Germany, these states mostly opted for the kinds of responses anticipated by my framework. They led internationally and protected democracy domestically. Germany stood out as an outlier among this group for giving less public voice to the Russian threat, balancing sanctions for the Kremlin's 2014 illegal annexation of Crimea with pursuit of increasing economic ties through projects like the Nordstream 2 pipeline.

But given its decades as ground zero for Cold War disinformation and espionage and its partition until 1989, there are pockets of significant Russian sympathy in Germany. A confluence of other factors including American dysfunction and unreliability likely account for a very pragmatic approach dealing with Russia. The other high will grouping was the closest fit with expectations.

High will and low capability states within my sample consisted of Australia, Finland, Lithuania, Netherlands, and Sweden. My framework expected these states to be innovators, maximizing limited resources by integrating societal responses domestically and seeking cooperative arrangements internationally. This group more consistently recognized the Russian threat as immediate and serious, driving innovative use of limited capabilities responding to Russian influence. They employed defensive alliances, total defense doctrines, and public education to protect themselves from Russia. These states supported democratic institutions and processes, built integrated resilient domestic responses, and generally punched above their weight addressing disinformation as a societal threat.

By contrast, Italy and the United States coded as low will and high capability. These two states largely acted in accordance with expectations, with some notable exceptions. I expected low will high capability states would show weakened or no state reaction to an external threat, employ state capabilities to spread disinformation domestically, backslide democratically, and polarize internally. Italy demonstrated all these predictions, but the United States' reaction was more mixed. Domestically, the United States acted more like a low will state backsliding and targeting disinformation at domestic audiences.

Internationally, however, its actions were more like that of a high will state leading international efforts to support democratic push back against Russia. This dynamic is explored in greater detail in the Chapter 5 United States case study.

Finally, my survey included two low will, low capability states: Poland and Spain. I expected little to no response by their state governments, leading to democratic backsliding and an attempt by other organizations to fill the void. These governments acted mostly according to expectations, focusing inwards even while the Kremlin attacked them from without. Both states suffered major declines in their democracies—Poland turned its state apparatus against its own people and Spain suffered a highly contested Russian-supported secession of a major subordinate region. There were also surprises studying these states. Mostly, that when external meddling is perceived as having gone too far, even low will states can quickly turn to addressing the threat.

Overall, the cross-national survey indicates of the two variables, will is more determinative of effective response to Russian disinformation. The high will low capability grouping, for example, were very active resisting Kremlin disinformation. Their elevated will drove integration of sectors across relatively small populations with weaker militaries. And their mixed histories with Soviet propaganda also yielded comprehensive policy approaches domestically and internationally. These states, though limited in resources, found creative ways to maximize those capabilities to fight disinformation more effectively than some high capability states. Further, states with low will struggled to find consistent, effective policies whether they were low or high capability.

Within groups of high or low will, a state's capability matters to the response. High will states had robust responses, but limited capability meant that the responses would be primarily diplomatic and defensive. High capability meant that the response would also include offensive actions to punish or disrupt Kremlin attacks. The two case studies provide greater context in this regard. The Finnish and United States Government are opposites in both will and capability. The case studies showed how their different endowments affected their responses to disinformation.

Finland

The Finland case study supports the importance of will and offers three main lessons: disinformation should not be considered in isolation from other aggressive influence tactics, Finland has found a way to maintain its high will in the face of Russian aggression, and what generates such high will in Finland may be impossible to repeat in other states. First, disinformation must be considered as part of a suite of capabilities that Russia employs to pursue it prerogatives internationally. The closer a state is located to Moscow, the more capabilities Russia uses to subvert it including not only disinformation, but energy policy, manufactured border crises, cyberattack, intimidation and threats, and even military invasion. Second, because it borders Russia and has long experience dealing with Soviet subversion, it highly attuned to the threat from Russian influence. Finland has invested in long term resilience emphasizing education of its citizens, coordination between public and private sectors, and trust and competence in its government leaders. The result is a stable society which maintains high will to resist Russian narratives. Finally, a close look at Finland shows that replicating its will against

disinformation may be impossible to replicate elsewhere. The country has a unique familiarity and skepticism from a century of near-constant struggle to balance asserting its democratic independence without triggering military aggression from Moscow. This struggle has imprinted deeply in Finnish society and cannot be quickly approximated in other contexts.

United States

My framework's predictions for the United States Government's response to Russian disinformation since 2013 was mixed. In some ways the response conformed with expectations. For example, Russian tactics employed within the United States have contributed to a decline in American democratic health. The last several years have seen multiple cases of disinformation intensifying divisions, fueling threats of violence against election officials, and motivating political violence at the Capitol. These trends are consistent with predictions of a state with great capability, but low will. By contrast, absence of unity in the United States system is not always evidence of absence of will. Because many of its world class state capabilities are foreign facing, my framework would better explain the United States' response if it made a clearer distinction between foreign and domestic spheres. For instance, the United States was highly engaged abroad helping other democracies providing intelligence to facilitate election protection. Domestically, though, political actors prevented government action during the 2016 election on intelligence that the Kremlin was interfering in our own elections. In a system inherently distrustful of government action domestically, especially in matters related to freedom of expression, American Civil Society Organizations (CSO) play a critical role

domestically. United States CSOs have been effective in exposing disinformation by attributing attacks, through investigative journalism, and in analyzing publicly available information. In many ways, the United States Government responded as a hybrid case: high will abroad, low will at home.

Chapter Outline

The rest of this work will explore these arguments and cases in detail. Chapter 2 outlines my framework centering on state will, capability, and how the combination of those two variables yields predictions about how government responses to Kremlin disinformation. Chapter 3 details the cross-national survey. It includes details on case selection criteria, measurements of will and capability, then discussion of how each grouping of states conformed (or did not conform) with theoretical expectations. Chapter 3 is supported by Appendix A which details findings for every state considered in my sample. Chapters 4 and 5 are case studies covering Finland and the United States, respectively, in greater context including Russian aims in attacking each. Finally, Chapter 6 summarizes the work including logical implications for the future of Russian disinformation targeting the West.

CHAPTER 2
CONCEPTUAL FRAMEWORK

Core Theoretical Argument

In this chapter, I outline my theory in greater detail to describe why different democracies respond differently to the threat of Russian disinformation. I am interested primarily in why states pursue different strategies and though there are myriad factors at play in an anarchic international political environment, a state's combination of capability and will broadly anticipate policy choices. I argue that both Russian employment of disinformation operations and the range of democratic states' response to those operations can be predicted through understanding balances of capability and will between democracies and Russia.

There is a wide spectrum of policy options available to combat disinformation. Some of the most common options I observed included weak responses like inaction, downplaying or ignoring the threat, or even amplifying Russian disinformation for domestic aims. More impactful responses included bolstering democratic norms domestically, enabling civilian sector organizations, updating laws aimed at slowing amplification and spread, clarifying false narratives, and educating the public. On the stronger end of the spectrum, actions like building coalitions to isolate Russia internationally, organizing sanctions, manipulating algorithmic promotion, and building new counter-disinformation organizations required significant will and capabilities. My expectation is that among states with comparable will and capability will select similar policy options. Below, I clarify what I mean by capability and will in the context of disinformation.

Capability

A state's capabilities responding to Russian disinformation results from different component elements of its power. There are several ways to determine a state's capabilities: some rough and some more precise. Important elements for responding to disinformation operations include Gross Domestic Product, cyber capabilities, geography, leadership and governance, economic power, industrial and technological capacity, military power, ideology, diplomacy, national character and morale, and foreign support. Among the countries I studied, for example, some are closer to Russia than others. Most are richer than Russia. Some are more capably governed and ideologically committed to democracy than others. Not all capabilities are particularly relevant to combatting disinformation. Raw military power or nuclear capability, for example, are not practically useful in fighting disinformation.

The menu of options available to each state responding to disinformation will derive from its capabilities. More capable states will naturally have more options from which to choose. In the extreme cases, a state with no capability can do nothing while a state with infinite capability can do anything it chooses. The states I have chosen all fall somewhere in between. Importantly, the states are sufficiently varied to yield meaningful conclusions from observing trends among the group.

As I will detail later, I sorted states by a combined measure of their capabilities. Aggregate capabilities are important, but do not tell a complete story; for that, we also need to consider disinformation-specific capabilities. A state's overall capabilities and its

capabilities in controlling information environments will determine its range of available responses.

Will

Like capability, a state's will is the manifestation of different component characteristics. Many different definitions of will exist. The operative definition for this work is that described in military conceptualizations of war, which describes that competition between two states is a "struggle between two hostile, independent, and irreconcilable wills, each trying to impose itself on the other."[27] Will is the commitment to seek policy preferences in a chaotic, competitive world while preventing other actors from imposing their preferences. From a Kremlin view, disinformation operations are meant to compete as intensely as possible without triggering a violent, damaging, and costly war which would run a risk of making Russia an international pariah.

Russia is employing disinformation to challenge the existing international system in ways that typically involved physical fighting to accomplish. Although in some cases Russia has in recent years invaded and occupied neighboring states, it has not invaded a major western democracy seeking to destroy its national capabilities or political system. Instead, it employs disinformation to weaken democracies from within. The tactics are different than popular imaginings of war, but the goals and some outcomes are similar. Russian disinformation challenges the existing world order by undermining democratic will in several ways.

27. See Marine Corps Doctrinal Publication 1: Warfighting.

Ben Nimmo has a helpful "four D" construct that describes how Russia employs disinformation. The four "Ds" are dismiss, distort, distract, and dismay:

> And for practically any event where the Kremlin or the Russian government is criticized you can be sure that they will do at least one of those four things. To dismiss they will insult the critics. The important words are "ignore them." It's all about dismissing the critic without looking at the evidence. Then distort; if you don't have the evidence that supports your story you make your own up. Distraction is the classic Soviet "what about you" technique—whataboutism—"So what if we are bombing Ukraine? You bombed Vietnam." And then dismaying tactics are you come out with lurid and terrifying hypotheses. "If you keep on doing this World War III will break out," but the idea is to say something so shocking and scary that people will actually back off and think "Whoa, do we really want to do this? Is this worth the risk?" Dismiss, distort, distract, and dismay.[28]

In different cases, Russia uses disinformation to impose its will on adversary states through narratives or reflexive control, creates space for maneuver by confusing adversary decision making, undermines faith in truth itself through whataboutism, and undermines morale through fear. All these effects are particularly dangerous to democracy which fundamentally depends on reliable information to enable effective collective judgements from which democratic regimes derive legitimacy. Undermining information, especially at critical points like elections, can change a result, affect policy, undermine faith in institutions, or force a state to turn inward away from Russian actions abroad. All of these are bad for democracy by undermining targeting democratic will.

In this dissertation, the concept of state will is the willingness to bear costs-- and to forgo potential benefits-- combatting the external threat from Russian disinformation. Will springs from factors such as perceived intensity and persistence of threat, unity and

28. See Haynes and Scott, Episode 2.

social cohesion, trust in government, structure of political system, elite behavior, partisan interests, and commitment to democratic norms. States that I considered are distributed on a spectrum of low to high will to fight Russian disinformation.

I expect states with high will to choose stronger and more comprehensive responses to the threat from Russia, but no state can have such high will that it can pay all costs and forgo all potential benefits to combat every potential threat. States must prioritize where it will exert will, as if each state had a "will budget" from which to draw. Varying history, geography, capability, and culture relative to Russia will determine how the Kremlin's potential threat rates among all potential threats, then would allocate commensurate will according to where Russia fit among its priorities.

Finland, for example, is a high will state which consistently prioritizes the threat from Russia. For more than a century, it has fought and competed against a much larger neighbor. It has lost territory and lives, at multiple times narrowly avoiding total domination from the Soviet Union. Although it has a long history of Russian, Soviet, and Russian again interference in its politics, it has firmly pursued an independent middle path between the West and Moscow. It borders Russia, it is much smaller, and it has fought wars of survival against Russia before. The threat to Finland, then, from Russia is direct, sustained, and existential so Finland's will remains consistently high.

A state with low will, especially those governed by leaders or parties who perceive a benefit from deploying disinformation, will do less or even nothing. Italy, for example, codes as low will. It has a history with Russia, even during the Cold War, that was more sympathetic and supportive than most other states in my sample. The Italian citizenry is

generally distrustful of its government, which has been led by some famously corrupt elites and pro-Kremlin propagandists. It does not share a border with Russia. The threat from Russian disinformation does not rank sufficiently high among Italy's security concerns to warrant paying the costs to combat it.

This is not to say that will is basically a function of whether Russian disinformation helps the political leader of a country in its domestic battles. While it may be the case that the Kremlin sometimes tries to get anti-establishment candidates into power, Russian operations are generally designed to support extreme candidates and conflicting positions on many sides of the same argument and to avoid discovery "until long after they are perpetrated, if they are recognized at all."[29] A candidate who takes office, even having been supported by Russian narratives in a campaign, is likely to be tarred as weak, corrupt, insane, and incompetent compared to more extreme options especially compared to Vladimir Putin.[30] Ultimately, the main side Russia takes in other countries' domestic battles is the one that most degrades consensus and formation of democratic will.

The level of will within a state generally will have predictable outcomes. High will states will perceive as serious and sustained the threat to democracy posed by disinformation. They will act not only to defend itself in the short term, but also seek to push back on purveyors of disinformation and work to elevate the threat perception of its allies. The low will states are likely to see the most pernicious effects of disinformation seep in, undermining the pillars of democratic governance intentionally or not.

29. Radin, et al., 2020, p. 3.
30. Gregor and Mlejnková, 2021.

The combination of these factors makes possible several predictions about whether a state will respond to disinformation and what types of options it is likely to choose if it

State Will: High	-State employs indirect (defensive) efforts. Examples: defense alliances, multinational institutions, public education campaigns, total defense doctrine -Protect democratic institutions/processes domestically -Build resiliency domestically -Integration among domestic sectors: government, media, society	-State employs mix of direct (offensive) and indirect (defensive) efforts. Examples: punish attackers, educate population, build and bolster multinational institutions -Protect democratic institutions, processes, and norms domestically and internationally -Leadership role integrating response to disinformation: domestically and internationally
State Will: Low	-State inaction; do nothing -Inchoate response by domestic sectors, limited to no role internationally -Democratic backsliding: institutions weaken, reduction in domestic freedoms and rights	-Weakened or no state reaction against external threat -Employment of state capability to use disinformation tactics against domestic audiences -Democratic backsliding: broken trust, institutions weaken, reduction in domestic freedoms and rights -Social division and struggle between domestic sectors, balance of power determines future direction
	State Capability: Low	State Capability: High

Table 1: Expectations by Will and Capability

does respond. Table 1 highlights the different expectations I have for each combination of high and low capability with high and low will. I will discuss each combination in the following pages.

Measuring Capability and Will

Measuring capability and measuring will require different approaches. Capability is a more clearly defined set of quantifiable characteristics and there are well developed indices. Capability is more stable than will. However, the capability of a state is useless without a will to make use of its powers. Will, therefore is not only the less stable factor, but also the more essential element of the two. This section outlines how I measure and compare state capability and will throughout this project.

First, capability is the simpler of these two variables to compare across states. There are several approaches already available to compare states to other states and to compare

states to themselves over time. Aggregate measures like Gross Domestic Product (GDP) are readily available and tracked over decades or even centuries. Big measures like GDP are rough. Measuring the output of a state is a way to consider its capabilities, but it lacks context. It is possible, for instance, to have a large state and a small state each with significantly different capability but equal GDP.

By contrast, other measures compare states with greater context. Michael Beckley, for instance, recognizing that GDP overstates the power of large states, proposes using GDP per capita (GDPPC)[31] to include consideration of not just a state's resources but also how efficiently it employs its resources.

At the root of Russian strategy to undermine democracy is its own realization that it is relatively weak relative to many leading democracies. Unable to compete successfully in a rules-based international order, Russia has adopted a zero-sum view of state power: whatever weakens its adversaries makes Russia stronger.[32] During the COVID pandemic, for example, as a NATO expert on Russian disinformation has written about vaccine disinformation:

> There's a reason why countries with which Russia has an argument find themselves facing public health crises because of well-funded and well-organized anti-vaccine campaigns. It is all just a measure to destabilize and erode and subvert adversary societies— not necessarily for any particular political outcomes. Because if you take as Russia does a zero-sum view of security then anything that you do to weaken your adversary, and that includes the United Kingdom, in relative terms makes you stronger."[25]

For my project, I believe a middle solution considering both a state's absolute

31. See Beckley, 2018, Unrivaled: Administering large states requires more overhead than governing small states. Additionally, corrupt and otherwise inefficient regimes consume more resources in running their states; this devalues rough measures of GDP since not all wealth created by a state is equally available for deployment.
32. Keir Giles, quoted in Haynes and Scott, Episode 2.

capability and specific information-related capability fits best. Overall capability is important, but the asymmetric nature of Russia's weaponized disinformation makes measuring specific capabilities important too.

I suggest an appropriate way to consider both aspects is in using two measures: the Correlates of War Project's Composite Index of National Capability (CINC)[33] and specific measures included in the Belfer Center's National Cyber Power Index (NCPI)[34]. The CINC shows states' general power relative to each other and over time by comparing more specific resource attributes than GDP.[35] And the NCPI is a composite score of several cyber capabilities among thirty different states. Although my interest is not cyber operations, some of the capabilities that the Belfer Center's index measures also bear on a state's capabilities to combat disinformation which is enabled and amplified through digital networks. Since my project focuses on 2013-2020, I will sort states primarily by their 2012 CINC scores relative to Russia. I will augment this general score with discussion of NCPI rankings for "information control" and "norms"[36] in the cyber domain, both of which are directly applicable to combatting disinformation.

---

33. See Singer, 1987. I used version 6.0 of the Correlates of War Project National Material Capabilities database which was published July 22, 2021. This database and covers the international system from 1816-2016 and is the basis for CINC.
34. Voo et al., 2020.
35. See Singer, 1987. The Correlates of War version 6.0 CINC Scores are annual measures from 1816-2016 for each state's share of total global material power. The index measures six factors: military expenditures, military personnel, energy consumption, iron and steel production, total population, and urban population.
36. Voo et al., 2020. p 19. The National Cyberpower Index defines Controlling and Manipulating the Information Environment as "Reflecting the duality of information controls, a country has prioritized using electronic means to control information and change narratives at home and abroad, AND/OR attempted to protect the internet privacy and free speech of its citizens. The form includes spreading domestic propaganda, creating and amplifying disinformation overseas, and using cyber capabilities to target and disrupt groups otherwise outside of its jurisdiction. The latter includes taking down extremist material from social media, and refuting foreign propaganda." It Defines International Cyber Norms and Technical Standards means: "A country has actively participated in international legal, policy, and technical debates around cyber norms. This might include signing cyber treaties, participating in technical working groups, and joining cyber partnerships and alliances to combat cybercrime and share technical expertise and capabilities."

In contrast, measuring will is much more subjective. Again, it is important to consider the aim of disinformation when thinking about how to frame a state's will to combat it. As Pomerantsev describes, Russia seeds disinformation to undermine trust in facts:

> Russian political parties are hollow and Russian news outlets are churning out fantasies. But insisting on the lie, the Kremlin intimidates others by showing that it is in control of defining 'reality.' This is why it's so important for Moscow to do away with truth. If nothing is true, then anything is possible. We are left with the sense that we don't know what Putin will do next—that he's unpredictable and thus dangerous. We're rendered stunned, spun, and flummoxed by the Kremlin's weaponization of absurdity and unreality."[37]

Undermining trust in facts degrades the ability to debate issues and solutions, in turn distorting or destroying collective decision making through majority rule, which is the essence of democratic governance. Combatting disinformation has two aspects: what a state does and what a state says. As mentioned previously, will springs from factors such as perceived intensity and persistence of threat, unity and social cohesion, trust in government, structure of political system, elite behavior, and commitment to democratic norms. There are publicly available databases that can measure some aspects of will including the Organization for Economic Cooperation and Development's measurements of people's trust in their national government. My project contributes measures of a state's will to oppose Russian disinformation by looking through publicly available government, media, and academic documents to determine individual states' history with the Soviet Union, and what states have done through policy to protect democracy from disinformation. These elements combine to describe why a state either did or did not perceive a threat from Russia and contribute to the intensity with which a state perceived

37. Pomerantsev, 2014.

that threat. The combination of trust, history, actions, and statements is used to measure the level of will each state brings to securing democracy from disinformation.

Since analyzing history, actions, and statements to derive a measure of trust would be its own project, I relied specifically on the Organization for Economic Cooperation and Development Trust numbers to sort states by will. For each of the thirteen states, I downloaded its rating for each year starting in 2012 and ending in 2020. Taking each state's average over that period and summary statistics of that sample, I sorted states into their respective quadrants quickly indicating a relative cross-national measure for the degree to which domestic populations trusted—and distrusted—their state governments.

Expectations

Low Will, Low Capability States

"If you want to boil a frog, you don't drop it in the boiling water because it'll jump straight out again. You put it in cold water, and you slowly bring the water up to boil. in doing so, by the time the frog realizes it's getting too hot, it's lost the energy to be able to jump out. We're being boiled like a frog." Lieutenant General Graeme Lamb.[38]

Expectations:
-State inaction; do nothing
-inchoate response by domestic sectors, limited to no role internationally
-Democratic backsliding: institutions weaken, reduction in domestic freedoms and rights

Because my project considers only wealthy and democratic states, states in my sample with low will and low capability are most limited. Other regime types derive their legitimacy from different power arrangements, but democracies depend more directly on popular support for state responses to Russian disinformation. This leads to several

38. Haynes and Scott, 2021. Episode 1.

predictions regarding their likely behavior and impacts felt within their democracies.

First, low will, low capability states are likely to do little or nothing to address the threat. States with low capability are typically smaller, less powerful democracies. Facing a threat from a larger adversary like Russia, these states are not powerful enough to push back directly. They may not even have capability enough to mount an effective defense. Small economies, small militaries, or weak cyber capabilities all reduce options available. These states are doubly unlikely to act because they lack the will. They may not perceive an intensity or persistence of a Russian threat. They may be especially divided or distrustful of government. The structure of their government may incentivize elites to ignore the threat or, more detrimentally, decide to adopt disinformation as a tool of domestic control. States with a mix of low capabilities and low will likely respond to disinformation ineffectively if it even chooses to respond in the first place.

A second prediction is that domestic actors sufficiently motivated by their threat perception will fill the void when they view their country is not sufficiently addressing the problem. These actors in weaker states will be generally ineffective since they lack the resources of a national government. Civil society organizations (CSO) are not large compared with states, but the same information environment that enables viral disinformation can correspondingly increase the reach of those who would resist. CSO will be unable to compel Russia to do anything. Still, their small size can incentivize innovation and flexibility. They can leverage international networks to influence domestic politics in the hope of preserving or building democratic values. I expect non-governmental entities within low will, low capability states to focus their efforts inward,

aimed at addressing their own governments, and not primarily fighting against foreign influence from Moscow. This creates a situation where the state and CSOs will be inwardly focused, unable, and unwilling to work with other states to generate international pushback against Russian interference. Such states will remain divided and vulnerable to effects of disinformation over time.

A final prediction is that when states do not act to mitigate the corrosive effects of disinformation, the campaigns will continue degrading the state's democratic institutions. Institutions will weaken and may even turn against domestic opposition and individual freedoms and rights will be curtailed. States with low capability and low will are likely to increasingly enact policies that advance anti-democratic aims which, intentionally or not, align with Russian strategic goals of weakening democracy globally. The states will be divided at home and will weaken ties between democracies internationally. Exact mechanisms of degradation within individual states will vary but will be mostly around key nodes of information processing and distribution effecting democratic functions: elections are likely to become less free, parties are likely to become more extreme, minority segments within the state's population will be targeted through legislation or courts, and dissent is likely to be punished using state power.

The saving grace of states with low capability and low will is that even if its leaders do choose to use disinformation as a tool for social control, it will be with considerably less effectiveness than a more capable state which decides similarly. Though they will have an inward focus, it will be with a less capable state apparatus power to instantly oppress its own people. But the Russian threat is external; low capability and low will

states are least likely to protect themselves from Russian disinformation and they are thus most likely to internalize the harms to democracy intended by foreign adversaries. These states are the frogs described above by General Lamb.

Low Will, High Capability States

"To put it bluntly, it's really hard— it's impossible— to excel at democracy and disinformation at the same time. Why? Because disinformation is designed to insidiously undermine the authority of the factual to undermine trust in institutions. And if you refine the capability of doing that to your adversary in the semi-covert way over years and decades then ultimately what history clearly shows is you will infect yourself. There's a blow back effect. You will start to believe in your own myths and your own constructions, as the Stasi called it, and the risk of self-disinformation if you do it for too long." Thomas Rid.[39]

Expectations:
-Weakened or no state reaction against external threat
-Employment of state capability to use disinformation tactics against domestic audiences
-Democratic backsliding: broken trust, institutions weaken, reduction in domestic freedoms and rights
-Social division and struggle between domestic sectors, balance of power determines future direction

I expect that low will high capability states will also struggle to internalize the external threat. To start with, these democracies are not short of policy options from which to choose. Being high capability means they are at least on par with Russia in terms of state power, and many democracies are much more powerful than Russia. If these states so chose, they have sufficient capability to apply offensive, defensive, unilateral, or multilateral responses to the problem. But, these states' plentiful resources make them better able to bear potential costs associated with confrontation. Where small

39. Haynes and Scott, 2021. Episode 2.

states' options are limited by capability, high capability states' choices are more likely to be limited by will. Whether these states intentionally underestimate the disinformation threat, seek to leverage the threat for domestic political reasons, or seek to ignore the threat all together, the results will eventually accumulate manifesting in the ways listed above.

Any actions a low will state chooses is likely to be ineffective against Russian disinformation. Russia has invested significant resources in weaponizing disinformation within an asymmetric hybrid warfare strategy. It knows it cannot compete with capable western democracies in a traditional confrontation, so it is pursuing an asymmetric challenge to the United States-led international order through nonconventional techniques of political warfare.[40] Democracies that underestimate the seriousness of that challenge do so at their own peril. These low will states will not organize sufficiently to match the intensity of Russian disinformation campaigns. This asymmetry allows Russia to operate at an advantage even within democracies that are more capable states. The effects of this dynamic are likely especially pernicious in more capable states than in less capable states.

Another likely response of a high capability low will to address Russian disinformation is highlighted by Thomas Rid's quote opening this section. This passage shows that such states risk self-disinformation. Although a powerful state's government may not have the will to use its capabilities combat Russian influence, those capabilities can be aimed at domestic audiences.

The techniques Russia uses to sow disinformation are not overly complex, but

40. Polyakova and Boyer, 2018.

they are effective attacks because they get right at the root of democracies. Disinformation undermines belief in facts as a way of kneecapping trust in institutions. Because institutions create fora for deliberation over time, healthy democracies will not employ disinformation. Doing so is counter to self-interest since it degrades the quality of collective decision making.

Anti-democratic elements within democratic societies, however, target dissolution of institutions. In capable states, there are tools and resources available to leverage disinformation techniques at home even if the state is uninterested in seriously countering influence from abroad. Like the low will, low capability states, this sets the conditions for disinformation to seep into a society.

Unlike the low capability states, however, the negative outcomes are likely to be more damaging if the tools are taken up by powerful actors. More capable states will be able to put greater resources into subversive efforts, further amplifying and disseminating attacks on institutions. Damage will accrue over time like collective body blows to a body politic: democratic backsliding, falling trust, weakened institutions, and curtailed rights will result.

Already existing social divisions within a capable state will widen and deepen. Once facts and arguments are devalued in debate and belief formation, what remains is spectacle and the raw power of might makes right.[41] This dynamic accelerates polarization and will eventually yield political violence if left unchecked for too long. This is the blowback of self-disinformation that Professor Rid describes above.

41. Snyder, 2017.

High Will, Low Capability States

"There are only two forces in the world, the sword and the spirit. In the long run the sword will always be conquered by the spirit." Napoleon Bonaparte

"We are on the front lines here. Brainwashing is a threat. If you are demotivating people, if you're spending fake news on whatever happens, if you are organizing referendum without informing people properly it's also a threat. You really can make big damage. This is not artillery, it's not conventional force, it's something else but it's very detrimental." Linas Linkevicius, foreign minister of Lithuania until December 2020.

Expectations:
-State employs indirect (defensive) efforts. Examples: defense alliances, multinational institutions, public education campaigns, total defense doctrine
-Protect democratic institutions/processes domestically
-Build resiliency domestically
-Integration among domestic sectors: government, media, society

States with high will and low capability are opposite of the high capability states with low will. Their lack of capability somewhat counterintuitively makes them more likely to push back effectively against Russian disinformation. These democratic states are relatively weaker than Russia. They have smaller economies, fewer people, and smaller militaries. This can predictably lead them to choose external balancing strategies to ensure state survival.[42] Building internal capabilities requires time and resources. In states which are dwarfed by Russia, choosing such a strategy could be futile; even if all resources a state could bring to bear were put against a Russian threat, they could still be insufficient to compete for survival. So, I expect the capability gap with Russia will lead these states to look for help externally through treaties, alliances, and cooperation.

Further, just as states with high relative capabilities may underestimate their

42. Waltz, 1979.

vulnerability to the threat of Russian disinformation, I expect that states with low relative capabilities will be more sensitive to the danger and perceive the threats from disinformation differently in both time and intensity. Small states will have fewer layers of institutions, competing power centers, myriad interests, and heterogeneous populations than larger states, which makes achieving consensus easier. Smaller states face less inertia and fewer collective action problems than larger states, requiring less time to achieve some sense of consensus recognition of a threat.

Smaller states are also likely to feel threats more acutely than powerful states. Smaller states have seen Russian aggression not only in other small states like Georgia and Estonia, but also repeatedly in large states like Ukraine[43]. Russian actions in those states have included efforts of redrawing borders in Europe through force of arms and military campaigns have been preceded by disinformation campaigns the forces in other wars have prepared areas with artillery or air power. The threat is more intense in smaller states on Russia's border which assess Kremlin aggression as potentially existential. The difference in threat perception is an important driver in generating will. Because threats are recognized faster and taken more seriously, I expect high will low capability states to pursue a rigorous strategy of self-defense and working with others to ensure survival.

As outlined above, I expect high will low capability democracies to respond to Russian disinformation through aggressively hardening their domestic capabilities while cooperating with other states to balance externally against a persistent threat by a more powerful adversary. Some more specific types of responses follow. I expect a low

43. Lucas et al., 2021.

capability high will state to innovate ways to become more effective through balancing. This can include not only participation in defense arrangements, alliances, and multinational institutions which counter Russian disinformation, but leadership in creating such arrangements and elevating awareness of the Russian threat. Because of the asymmetry in the intensity and duration of threat perception between small states and large states, I expect that small states will be more motivated than larger states to rally as many external capabilities as possible to response. Additionally, I expect that small states will respond more aggressively within their borders to harden themselves against attack. Defense doctrines, public education campaigns, legal structures, and formation of governmental organizations, for example, are likely options for these states to pursue.

Domestically, defensive strategies pursued by states relatively weaker than Russia will include bolstering institutions, building resilience among the population, and integrating different societal sectors to resist the corrosive effects of disinformation. Because Russian aims are to undermine democratic institutions, small states with a will to resist will likely act to shore up their domestic democratic institutions. Elections and political parties are key areas where Russian influence can change the internal dynamic within democratic states. Low capability states will make efforts to defend them.

Also, small states with high will will build resilience within its population to the individual level. Digitally enabled Russian influence operations are aimed at individuals to sow division. Cell phones and web browsers can put disinformation directly in front of individual citizens; a coordinated defense will include training and education programs for detecting disinformation and blunting its effectiveness. Finally, coordination between

sectors should be more readily apparent in smaller democracies. Just as small states will seek to defend through leveraging international cooperation, they will also organize internally to mitigate disinformation. I expect that there will be coordination between government, civil, and media groups working together against Russian meddling. Because these states have high will, there will be more extant trust in institutions and government or other characteristics that make unity of effort more achievable.

Because high will states will integrate their international and domestic efforts, I expect they will be more effective in pushing back against Russian disinformation. The threat posed will be perceived earlier and taken more seriously because it comes from a relatively more powerful adversary. The combination of low capability and high will forces these states to find creative responses, making them innovators.

High Will, High Capability States

"What they mean by unresolved contradictions is frictions, for example nascent antisemitism in Germany in the 1960s or unresolved racial tensions in the United States also in the 1960s or even today, and then designing and driving a wedge into those cracks in order to pry them open— for example to drive a wedge between West Germany and the United States or between NATO allies."[44] *Thomas Rid*

Expectations:
-State employs mix of direct (offensive) and indirect (defensive) efforts. Examples: punish attackers, educate population, build and bolster multinational institutions
-Protect democratic institutions, processes, and norms domestically and internationally
-Leadership role integrating response to disinformation: domestically and internationally

In states with high will and capability, all options of response are available. These

44. Quoted in Haynes and Scott, 2021. Episode 2.

states come to conflict with Russia with equal or greater state capability. This offers opportunities unavailable to smaller states similarly disposed to counter Russian disinformation. But the pairing of high will with high capability is a double-edged sword. On one hand, these states are likely to be among those most targeted by Russia because the attacks can have the highest payoff degrading democracy globally. On the other, these states are most capable in pushing back against disinformation and can impose large costs against Russia for its efforts.

The high will high capability states are likely to be most targeted because Russia's strategic goal is challenging the postwar democratic world order. As discussed, Russia's challenge is posed by degrading that order by weakening ties between democratic states globally and attacking individual states to degrade democratic states domestically. The high capability states in this grouping will be targeted more because they are leading democracies internationally. Therefore, the payoff for weakening a big democracy is increased: weakening an individual state is good, but driving a wedge between a multinational organization like NATO, designed to contain Soviet power after World War II and refocused after the Cold War on expanding further into Russia's sphere of influence, is much better.

High will high capability states will also include many democracies which are more capable than Russia. Russia does not employ disinformation because it is strong; Russia employs disinformation as an asymmetric tactic to close a growing capability gap with rich democracies. These states should be motivated to respond. While low capability states are highly motivated by costs since they face potential threats to their survival, high

capability democracies are those that have reaped the most benefit from the postwar international order. Disruption to that order will manifest as serious costs in rich democracies. So, differently than its use in smaller states, in powerful democracies Russia does not use disinformation from a position of strategic strength, but one of strategic weakness. Excepting the use of its nuclear weapons, Russia does not have sufficient capability to pose an immediate existential threat to this group. This impacts how these democracies perceive the threat and drives a different set of expectations for their responses.

Among the four categories of democracies, this group should be expected to be the most active in dealing with Russian disinformation. They have sufficient capabilities to push back directly against Russia if they choose. They also can coordinate and lead other states in opposing Russian interference. This should manifest in high capability, high will states opting for a mix of both approaches acting with allies when possible and unilaterally when necessary.

Second, because the most capable democracies have benefitted most from the postwar international order, they have more to lose to the degree Russia and other challengers to that order are able to undermine that order. This leads to the other expected types of responses from this group of democracies. They are likely to bolster the key institutions targeted by disinformation campaigns. These institutions are not only the recurring venues and international bodies where repeated interactions between states drives geopolitics, [45] but also the embedded norms that have allowed democracy to thrive

45. Keohane, 1984.

internationally.[46]

The most likely areas to protect in democracies are the most vulnerable: free elections, rule of law, anti-corruption, and free expression. Different states will protect these institutions and values differently, but these areas are simultaneously what makes democracy function and potential vectors for disinformation to corrode governance most effectively from within. In addition to protecting institutions and norms domestically, the high capability, high will democracies will also be those leading efforts between democratic states in promoting democracy internationally.

The low capability, high will states may be entrepreneurs that innovate and elevate potential solutions to combat disinformation, but it is high will, high capability states that will get engaged to scale responses to powerful groups of states. Once engaged, the capabilities these states can bring to bear are each greater than Russia can muster. In concert with others, the collective capabilities of big democracies dwarf Russian state power.

The goal of Russian strategy is to push just hard enough to undermine its enemies without precipitating a forceful response from more powerful international actors. Again, this is a strategy favored by the weaker state in an asymmetric competition. States with high capability and high will face the biggest potential costs of disruption to the international order, can counter Russian influence domestically, and have the power to lead internationally. It is these states which will be decisively succeed or fail to secure and promote democracy in the face of threats from Russia.

---

46. Ruggie, 1982.

Conclusion

In conclusion, my theory is that different democratic states should be expected to respond to Russian disinformation operations according to each state's mix of capability and will. Between capability and will, capability will be more stable and easier to measure. A state's capability determines the range of policy options available to protect democracy both domestically and internationally. However, it is will that is the more important factor. If capability determines the options available, it is only through will that a state will choose and sustain a set of policies to fight against a relentless flood of disinformation. Russia is a large state with considerable capabilities, especially in conducting deliberate disinformation operations to undermine the United States led international order. The range of expected responses should break down along states with high or low capability and high or low will.

Low capability, low will democratic states will do little to nothing against the external threat. They will be the most susceptible to the corrosive effects of disinformation. High capability, low will states will also fail to defend themselves effectively but because they are relatively powerful, run the risk of self-disinformation if capable powers within the state use disinformation as a tool of internal control. In both low will groupings, the rights and protections of domestic actors will erode.

Low capability, high will states will be highly sensitive to the threat of disinformation from Russia. Their relatively small size will make them sensitive to external aggression leading to a sustained, possibly existential threat. This perception will lead to innovative solutions. Plus, these small states will be advocates for elevating the threat among other

democracies to balance. Finally, high capability, high will states will be the decisive group in determining how effective democracies will be in countering the disinformation component of Russia's strategy undermining the global order. These states will likely be less sensitive to the threat since they are likely to overlook a relatively less powerful Russia, but these states also have the most to lose. If they realize the threat in time to sustain their will, these states have the power to punish Russia unilaterally and the influence to organize collective response by democracies internationally.

The next chapter will show how this dynamic unfolded among a select group of democracies from 2013-2020, a period when Russia significantly escalated its employment of disinformation supporting aggressive military invasions into neighboring states and hybrid political warfare interfering with several other states, including leading global democracies.

CHAPTER 3
CROSS-NATIONAL SURVEY

Introduction

The Russian escalation after 2013 seemed in some ways like a random flood of sometimes ridiculously unbelievable lies. But the operation was far from random. Instead, it was a highly tailored global influence campaign against the democratic world order. The operation had specific objectives, key among them was maintaining power in Russia.

As Lucas et al describe, this strategy is meant to maintain stability domestically while creating or threatening instability abroad:

> The Russian regime's foremost interest is its own hold on power. All policy, internal and external, stems from this overriding goal. The Kremlin sees the West, the European Union (EU), and NATO as threats to this stability, and as potential instigators of "color revolutions" that will exploit Russia's ethnic, religious, political, and other fissures. The long-term goal is, therefore, a polycentric or multipolar world in which multilateral, rules-based organizations are unable to dictate terms to Russia. Instead, the Kremlin aims to be the dominant power in Eurasia, using Russia's size to exert strong influence over its neighbors and over small countries, and to bargain with big countries on an equal basis.[47]

To bring about its goal, Russia began in the mid 2000s a series of campaigns against Georgia, Estonia, Ukraine, and other neighboring states that included further adaptation of information warfare to advances in digital technology. By 2013, the Kremlin had been experimenting for a decade on how to employ disinformation in what many claimed was a new form of hybrid war. According to Peters, the invasion in Ukraine was proof of concept for new applications of Soviet techniques like:

47. Lucas et al., 2021.

> denial and deception, concealment of the Kremlin's goals, 'retaining superficially plausible legality,' using threats of military power and using threat of nuclear weapons, deployment of resources globally and through social media a recrafting of the narrative of conflict.[48]

Recrafting the narrative is meant to generate disorganization and disunity within foreign competitors.[49] At the time, the United States' Supreme Allied Commander Europe declared invasion "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[50] For the first months of the operation, Ukraine was the main target of Russian disinformation. That soon changed as the operation expanded to attack the United States and most states in the European Union and NATO.

Adapting Soviet tactics and with a goal of subverting the West, the Kremlin used new tools of a networked world to gain unprecedented dissemination of propaganda. Freed from any desire to bring recipients along with a movement in the direction of global communism, Russia instead just started sowing doubt within and between democracies using a far-reaching army of trolls, bots, social media, and fake websites. Now, as described by Bola and Papadakis, the digital propaganda employed against the West since 2013 "works differently. It is primarily interested in the destruction of the epistemological foundation that informs the process of validation and adjudication of claims of political relevance for the constitution of contemporary societies."[51]

In this new context, contaminating global information flows with lies is not a bug, but a feature designed to advance Kremlin objectives by distracting and confusing its

48. Peters, 2017.
49. Pynnöniemi and Rácz, 2016, p. 33. "The Soviet and subsequent Russian approach to strategic deception can be explained with three different but complementary concepts: organizational weapon, reflexive control and active measures."
50. Vandiver, 2014.
51. Bjola and Papadakis, 2020, p. 639.

democratic adversaries.[52] This chapter seeks to understand what different states did in response during the operation. Some did a lot. Others did nothing. As described in the previous chapter, I argue that a combination of democratic states' will and capability drive their policy responses. In this chapter, I draw on the experiences of thirteen democracies targeted by Russia from 2013-2020 to test that argument.

Selection of States

Before comparing what western democracies did to combat Russian disinformation, I applied several screening criteria to define what subset of states to consider. Three criteria yield thirteen democracies most relevant to studying state-level responses.

First, my interest was in studying democracies. The Economist Intelligence Unit (EIU) annually ranks democracies according to 60 indicators of electoral process and pluralism, civil liberties, functioning of government, political participation, and political culture. Scores in those categories are then adjusted if a country does not get a full score for free and fair national elections, voter security, foreign influence in government, and civil service capability. Each country then gets ranked as a full democracy, flawed democracy, hybrid regime, or authoritarian regime.[53] In the 2020 rankings, 75 national governments scored as full or flawed democracies.

Second, although there are several states employing disinformation campaigns to influence foreign audiences and elections, this project focused on Russian disinformation. As such, screening for NATO countries made sense. NATO is a decades old military

52. Pynnöniemi and Rácz, 2016, p. 17-18. "openly false, rapidly varying Russian communication is aimed not at convincing the decision-makers, but at dazzling the public audience by providing numerous alternative narratives to the Western ones… the main objective of these measures is to dazzle and disorient."
53. Economist Intelligence Unit Democracy Index 2020, p. 56-57.

alliance established after World War II to contain the Soviet Union. Since the end of the Cold War, the alliance has refocused, expanding to include several former Soviet Republics and Satellites, and the alliance continues to contain Russia. In addition to formal signatory member states, however, I also consider five countries who are NATO Enhanced Opportunity Partners. Enhanced Opportunity Partners, several of which are very near Russia, have privileged relationships protections under NATO despite not being treaty signatories. Part of the reasoning for Enhanced Opportunity Partners is to coordinate multinational responses to hybrid and new threats. This includes information warfare, which Russia has accelerated and intensified in the early decades of the 21st century. Including Enhanced Opportunity Partners offers a fuller picture of responses to Russian aggression. The list of full or flawed democracies which are NATO members or Enhanced Opportunity Partners narrowed the Economist Intelligence Unit list to 30 countries.

Third, I focused on the 13 of these 30 states publicly known as targets for Russian influence efforts. Martin, Shapiro, and Ilhardt have studied nearly 1000 media reports on state sponsored attempts at foreign influence using coordinated disinformation campaigns. They identified 76 foreign influence efforts between 2011 and 2020. Of those, 64% emanated from Russia and most targeted NATO and Enhanced Opportunity Partner democracies.[54]

I scoped this even more narrowly, focusing on 2013 to 2020. This period coincides with Russia's invasion into Ukraine and ends with the World Health Organization's

54 Martin et al., 2020.

declaration of COVID-19 pandemic. The invasion into Ukraine included an unprecedented escalation of Russian information operations which had been honed in earlier attacks on Georgia, Estonia, and others. The escalation continued to involve attacks on elections and democratic norms in democratic states and between democracies internationally.

The COVID pandemic marked a new opportunity for more actors, having seen the impact of Russia's campaigns, to adopt disinformation techniques exacerbating divisions. By then, however, governments had had time to study, understand, and respond to disinformation. I aimed to study what different states did during that recent explosion of aggressive information operations. Using Martin, Shapiro, and Ilhart's foreign influence efforts database, 13 NATO and Enhanced Opportunity Partner states are publicly known to have experienced Russian disinformation campaigns at least once

EIU ranking 2020	Country	Regime type	NATO+EOP	Attacks by Russia 2013-18
25	United States	Flawed democracy		14
16	United Kingdom	Full democracy		3
9	Australia	Full democracy		2
14	Germany	Full democracy		2
9	Netherlands	Full democracy		2
5	Canada	Full democracy		1
6	Finland	Full democracy		1
22	Spain	Full democracy		1
3	Sweden	Full democracy		1
24	France	Flawed democracy		1
29	Italy	Flawed democracy		1
42	Lithuania	Flawed democracy		1
50	Poland	Flawed democracy		1
7	Denmark	Full democracy		
2	Iceland	Full democracy		
13	Luxembourg	Full democracy		
1	Norway	Full democracy		
71	Albania	Flawed democracy		
36	Belgium	Flawed democracy		
52	Bulgaria	Flawed democracy		
59	Croatia	Flawed democracy		
31	Czech Republic	Flawed democracy		
27	Estonia	Flawed democracy		
37	Greece	Flawed democracy		
55	Hungary	Flawed democracy		
38	Latvia	Flawed democracy		
26	Portugal	Flawed democracy		
62	Romania	Flawed democracy		
47	Slovakia	Flawed democracy		
35	Slovenia	Flawed democracy		
18	Austria	Full democracy		1
45	South Africa	Flawed democracy		1
49	Brazil	Flawed democracy		1
4	New Zealand	Full democracy		
8	Ireland	Full democracy		
11	Taiwan	Full democracy		
12	Switzerland	Full democracy		
15	Uruguay	Full democracy		
17	Chile	Full democracy		

Table 2: Selection Criteria for States in Cross-national Survey

from 2013 to 2020.[55] Of course, it bears noting that because of attribution problems, there almost certainly have been attacks which are not publicly known.

The multiple screening criteria resulted in a list that includes the United States plus 12 other democracies, each in formal security agreements with the United States, and each known to have been attacked by Russian disinformation in recent years. This list is shown in Table 2.

Methodology

For this chapter, I relied on grounded theory looking at actions taken by a select group of democracies and coding their responses at a state level through a specific period. I used the data to test my theory that capability and will cause different states to respond differently.[56] As a starting point, Martin, Shapiro, and Ilhardt's database of Foreign Information Efforts (FIE) was useful. The database provides rich contexts about various operations conducted from 2013-2018, including numerous characteristics of attackers, actors, strategies, platforms, sources, approaches, tactics, and topics.[57] They detail FIEs from the attackers' perspective. My contribution is to explain the flip side of those efforts, creating a list of broadly corresponding characteristics of responses taken by the targets of FIEs— specifically Russian FIE. Because of the dual nature of conflict, many of the same categories of variables that describe an attack can be reversed to describe a corresponding defense or countermeasure.[58] I relied on official documents and publicly

55. Martin et al., 2020.
56. Ravitch and Carl, 2021.
57. Martin et al., 2020.
58. Marine Corps Doctrinal Publication (MCDP) 1, "Warfighting"

accessed documents including books, government documents, chapters, journal articles, blog posts, and press reports to describe each states' actions.[59]

None of what I reviewed is classified. Although specific operations are classified, my interest is in the broader strategic and societal impacts of disinformation. Assessing this does not require access to anything not publicly available. In fact, because I was interested in the responses to disinformation, I believe it was better to focus only on public reports. Main goals of Russian disinformation include disorientation, distrust, and confusion. Muddying the water and making all information seem untrustworthy is an end.[60] That goal is accomplished across society, not limited to the halls of the Pentagon, State Department, or Congress. Public acceptance of false narratives or of preventive measures meant to combat disinformation mainly determines of how corrosive disinformation will be within a society. So, publicly observable actions are what really matters.

This approach did risk blind spots, however. Not only did I not consider classified information, but also disinformation often relies on anonymity or misrepresentation of sources. Skilled propagandists exploit media biases for elite institutional focus, headline seeking, and neutrality[61]. This required other methods besides analyzing press reports to ensure an accurate description of democratic responses. I used several different sources and methods to enhance the validity of this survey. This helped ensure that my findings presented a layered, coherent interpretation of state-level responses. I used a mix of

59. Ravitch and Carl, 2021.
60. See Snyder, 2017 and Pomerantsev, 2019.
61. Benkler et al., 2020.

documents, expert testimony, practitioners from different states, and a wide range of publications over nearly a decade. This ensured I was not seeing the phenomenon through the limited perspective of one individual, source, or time. [62]Interestingly, during this study I came across a breadth of perspectives that was wide enough to include articles which themselves voiced Russian propaganda. I discarded sources that made demonstrably false claims like Russia had not invaded Ukraine. I will not cite that source here to avoid amplifying falsehoods.

I also worked to account for two blind spots resulting from my sample of states. First, I acknowledge that the sample consisted of a small group of exceptional states—Western democracies in some level of formal security relationship with the United States and which have been attacked by Russian disinformation since 2013. Within this small group, however, I believe there was a sufficiently wide range of population, size, historical context, legal systems, institutions, traditions, and geography to draw valid conclusions about capabilities and will as variables that shape how states responded to disinformation.

Second, I only worked in English. Because disinformation adapts to changing contexts, language can be an important screen; some of the smaller states with their own languages have an advantage when non-native speakers attempt to push disinformation. Grammatical errors can sometimes be easy flags that call into question a message's authenticity. This raises the bar for narratives to penetrate information filters, especially in a small state with a distinct language like Finland. I tried to mitigate this by looking at sufficiently broad accounts from multinational sources like NATO documents, which are

62. Ravitch and Carl, 2021.

compiled by experts who regularly work in multiple languages, and English translation of foreign documents.

To structure my collection of evidence, I developed a codebook detailing state level governmental actions taken from 2013-2020. I had one codebook per state, covering responses to specific attacks and general approaches to managing the information environment. Typical responses included education campaigns, changes to election law, and updated media practices meant to deal with disinformation.

This study was inductive. I learned through the process and adapted the codebook after completing each of the first several states. Given its small size and my language limitations, I started with Lithuania to determine feasibility of collecting data on my sample. I analyzed the collected data at each step of the project to ensure there was sufficient information to support conclusions.[63] Collecting sources for each state provided iterative opportunity to refine the codebook as a collection instrument. That required me to also update past instruments before moving forward. After collecting data, I grouped the states into groups according to their level of will and capability as outlined in Chapter 2. I include narrative summaries of each state in Appendix A. In the next section of this chapter, I will outline my findings by states grouped according to will and capability.

63. Maxwell, 2013.

Findings

Low Will, Low Capability: Poland, Spain

Coorelates of War CINC			NCPI Ranking (Information Control and Norms)			OECD Trust		
	Avg. 2013-16	Since 1991	State	Average		State	Average	
United States	0.13204	Q1	United States	1.0	Q1	Netherlands	61.31	Q1
Russia	0.03786	Max .15630	United Kingdom	7.0		Germany	58.83	Max 80.86
Germany	0.01688	Q2 .01998	Russia	7.5		Canada	58.02	
United Kingdom	0.01433		France	10.0	Q2 9.4	Finland	57.01	
France	0.01374		Australia	11.0		Sweden	55.48	Q2 55.73
Italy	0.01150		Sweden	11.0		Russia	51.57	
Canada	0.00861	Median .01040	Canada	12.5		Australia	45.66	
Spain	0.00764	(Q3 .02281)	Netherlands	14.0	Q3 12.8	United Kingdom	40.42	Q3 44.92
Australia	0.00674		Germany	15.5		France	36.22	
Poland	0.00549		Spain	17.5	Q4 16.0	United States	35.09	
Netherlands	0.00398	Q4 .00543	Lithuania	22.5		Lithuania	33.86	Q4 34.52
Sweden	0.00210	min .00039	Italy	24.0		Poland	33.11	Min 14.57
Finland	0.00151					Spain	29.10	
Lithuania	0.00041					Italy	25.19	

Table 3: Ratings for Low Will, Low Capability States

			Expected Action		
Legend:			State inaction; do nothing	Poland	Spain
Observed	Low Will	Low Capability	Inchoate response by domestic sectors, limited to no role internationally	Poland	Spain
Inconsistent			Democratic backsliding: institutions weaken, reduction in domestic freedoms and rights	Poland	Spain
Not observed					

Table 4: Overall Findings for Low Will, Low Capability States

According to my framework, there are two low will, low capability states in the sample: Poland and Spain. As shown in Table 3, these states are both in the lower half of average CINC scores from 2013-2016. Spain is in the lowest quartile of the Belfer Center's NCPI rankings for Information Control and Norms. Yoo et al. did not even rank Poland in its measure of national cyber powers. And both states were in the bottom three rankings for Organization for Economic Cooperation and Development Trust scores. They are two of the least capable, lowest will states according to my selected measures.

As low will low capability states, my theory predicts that they would be inwardly focused with a weak state apparatus not oriented on protecting itself from the threat of

external Russian propaganda. I also expected that these states would be most likely to internalize the harms to democracy intended by foreign adversaries. I saw evidence that mostly supported these expectations and the policy choices I thought would result: that the state governments would mostly do nothing about Russian disinformation, that there would be an inchoate response by domestic sectors trying to address vulnerabilities, and that there would be corrosion of democratic norms within the states. These findings are shown in Table 4.

Both Spain and Poland ignored Russian disinformation and focused domestically. Spain eventually named Russia for meddling in Spanish domestic politics, but not until years of choosing to talk about disinformation without directly accusing Russia.[64] Poland also focused internally. Its ruling party, PiS or Law and Justice, focused its efforts on undermining its domestic political opposition, demonizing immigrants, and promoting nationalist policies.[65] In the face of government inaction, particularly in Poland, civil society organizations (CSO) did organize to address disinformation. Dozens of organizations sprouted some directly inspired by Ukrainian organizations that had stood up to combat Russian disinformation. The growth in the number of CSO forming in Poland accelerated early in the period, peaked at 14 in 2017, but tapered off dramatically as Law and Justice consolidated power. By 2019, no new CSOs were established.[66]

Spain and Poland also both saw significant democratic backsliding. As Law and Justice consolidated power, it continued ignoring Russian disinformation and took its

64. Jopling, 2018.
65. Gregor and Mlejnková, 2021.
66. Ibid.

own actions to weaken democratic norms domestically. The government fired and harassed hundreds of journalists, employed botnets and troll farms in elections, and turned public media into a party propaganda outlet.[67] As a result, Poland has effectively become a one-party state and slipped dramatically in press freedom rankings.[68]

During the period, Spain also backslid. In 2017, there was a vote for Catalonia to secede from Spain. This was a highly divisive issue that Russia exploited and exacerbated. The vote for secession prompted strong reaction from the national government which jailed some opposition politicians, dissolved the Catalan government, and instituted direct rule from Madrid.[69] This is a serious degradation of democracy—both in splitting a state and then in jailing opposition leaders while disbanding subordinate governments. The inward focus of Poland and Spain, plus the resulting curtailment of domestic freedoms are all consistent with predictions. I also found evidence of reactions that my framework did not anticipate.

Poland and Spain both defied predictions in limited incidents. For example, at a time while the Polish government was using disinformation against its own people, they also contributed senior level employees at NATO's Strategic Communications Center of Excellence (StratCom CoE).[70] That organization's mission is to coordinate NATO narratives, founded during Russia's initial invasion of Ukraine, and so can be seen as a response to Russian information operations. This exception may be due to timing, however. The Center of Excellence was established in 2014 while Law and Justice was

67. Kosc, 2020.
68. Ibid.
69. Minder, 2019.
70. Gregor and Mlejnková, 2021

still a minority party in Poland. Law and Justice only became Poland's governing party in 2015. Perhaps after Law and Justice took power, Poland would not have been such an active participant in a multinational counter-disinformation effort.

Spain also challenged my assumptions. As mentioned, early in the period I saw no evidence of Spanish state concern for Russian disinformation. That changed with the Catalan independence vote; by 2017, Spain reorganized its defense strategy acknowledge Russian disinformation. It also called out Russia for election meddling during European Union elections.[71] I underestimated low will low capability states' potential to regain focus so quickly. Acceptance of the threat cannot come too soon; as COVID bookended the period of my exploration, Spain was an early pandemic target of medical disinformation. Further study can add to understanding whether Spain adapted better counter-disinformation policies after the Catalan secession and European Union election lessons.

In conclusion, the low will low capability states largely conformed with what I expected to see. The Polish and Spanish Governments were inwardly focused even while Russian attacked them from without. Both states suffered major declines in their democracies— Poland turned its state apparatus against its own people and Spain suffered a highly contested Russian-supported secession of a major subordinate region. There were also surprises studying these states. Mostly, that if and when external meddling is perceived as having gone too far, even low will states can quickly turn to addressing the threat.

71. Booth and Birnbaum, 2017.

Low Will, High Capability: Italy, United States:

Coorelates of War CINC			NCPI Ranking (Information Control and Norms)			OECD TrUnited Statest		
	Avg. 2013-16	Since 1991	State	Average		State	Average	
United States	0.13204	Q1	United States	1.0	Q1	Netherlands	61.31	Q1
Russia	0.03786	Max .15630	United Kingdom	7.0		Germany	58.83	Max 80.86
Germany	0.01688	Q2 .01998	Russia	7.5		Canada	58.02	
United Kingdom	0.01433		France	10.0	Q2 9.4	Finland	57.01	
France	0.01374		Australia	11.0		Sweden	55.48	Q2 55.73
Italy	0.01150		Sweden	11.0		Russia	51.57	
Canada	0.00861	Median .0104	Canada	12.5		Australia	45.66	
Spain	0.00764	(Q3 .02281)	Netherlands	14.0	Q3 12.8	United Kingdom	40.42	Q3 44.92
Australia	0.00674		Germany	15.5		France	36.22	
Poland	0.00549		Spain	17.5	Q4 16.0	United States	35.09	
Netherlands	0.00398	Q4 .00543	Lithuania	22.5		Lithuania	33.86	Q4 34.52
Sweden	0.00210	min .00039	Italy	24.0		Poland	33.11	Min 14.57
Finland	0.00151					Spain	29.10	
Lithuania	0.00041					Italy	25.19	

Table 5: Ratings for Low Will, High Capability States

			Expected Action		
Legend:	Low Will	High Capability	Weakened or no state reaction against external threat	Italy	USA
Observed			Employment of state capability to use disinformation tactics against domestic audiences	Italy	USA
Inconsistent			Democratic backsliding: broken trust, institutions weaken, reduction in domestic freedoms and rights	Italy	USA
Not observed			Social division and struggle between domestic sectors, balance of power determines future direction.	Italy	USA

Table 6: Overall Findings for Low Will, High Capability States

Of the thirteen states in my sample, Italy and the United States coded as low will and high capability. My framework expects these countries to experience widening and deepening social divisions as domestic elements compete in a more post fact and post truth information environment. As mentioned previously, once facts are devalued within democratic debate and belief formation, what remains is attacking people who hold opposing beliefs.[72] This dynamic accelerates polarization and will eventually move beyond words to political violence if left unchecked for too long.[73] The two states largely conformed to my expectations that low will high capability states would show weak or no

72. Snyder, 2021.
73. Mason, 2018.

state reaction to an external threat, employ state capabilities to spread disinformation domestically, backslide democratically, and polarize internally with increasingly divergent groups competing for power. Italy demonstrated all these predictions, but the United States Government reaction was more mixed.

Italy and the United States, while both grouped as low will and high capability as reflected in Table 5, are quite different from each other. Both are among the most powerful states as ranked by CINC score. The United States for this period was still far and away the world's most capable democracy with an average of 13% share of global power according to CINC metrics. Italy, while still above average even among this group of mostly rich Western states, still averaged about one tenth of the United States' overall capability at 1.1% of global material capability. In addition to that gap, the Belfer ranking for Information Control and Norms ranked the United States first and Italy last among my sample. The United States' ranking is somewhat misleading, however, since it was earned by virtue of its efforts combatting Islamic State influence. The United States, then, demonstrated success combatting narratives in a contested environment, just not necessarily in a domestic environment being challenged by Russia. In other words, when the United States had the will to disrupt and degrade Islamic State influence, it did so. Its will to respond to Russian attacks was less clear. These high capability states did not demonstrate will to respond to Russian disinformation throughout the period and so my framework largely predicts what resulted.

Table 6 shows that responses to Russian disinformation in the United States and Italy conformed with my expectations. First, each showed weakened or no state reaction

against the external threat. Italy has a long history of close support for Russia. Even during the Cold War, it had the largest Communist Party in Western Europe. Now, in a post-Soviet era, it still has segments of pro-Russian sympathy, especially in the Five Star movement that led Italy for much of the period under consideration.[74] And in a Trump-led United States, even the significant efforts the United States Government eventually took to address Russian meddling was despite, not because of, Presidential leadership. This muted the response from the world's oldest democracy.

Second, both states' ruling parties employed disinformation tactics against domestic audiences. The Italian former Deputy Prime Minister Matteo Salvini, for example, spread disinformation, including pro-Putin disinformation, and used to build his official campaign website the same propagandist who built other sites including "I'm with Putin," and "StopEURO."[75] In the United States, Donald Trump long dabbled in conspiracy theories including questioning President Obama's citizenship, campaigned while enabling Russian interference, and used social media during his administration to spread conspiracy theories aimed at undermining the legitimacy of his critics and opponents.[76]

Third, democratic backsliding occurred in both states over this period. And elections have turned into a tribal competition for power rather than a competition of policy differences. Trust in government among Italian citizens is generally low and they recorded the lowest score of any annual measure among the sample for my period; in

74. Christiani, 2020 and Weiss, 2020.
75. Appuzo and Satariano, 2019.
76. Benkler, 2018.

2013, only 14% of Italians voiced trust. By the end of the period, the government justified this lack of trust, releasing previously classified intelligence that showed the government knew Russia and China had been interfering in their democracy.[77] Democracy in the United States also backslid. Its ranking in the Economist Intelligence Unit and other methodologies no longer classify the system as a full democracy.[78] President Trump systematically sought to undermine the legitimacy of elections by spreading disinformation about voting fraud, stoking conspiracy theories, and even kneecapping the post office.[79] Former President Trump's party has not developed a party platform since the 2016 election, instead relying on nativist and nationalist appeals to a base, amplifying lies, conspiracies, and threats of violence not to win a battle of ideas within a political framework, but to motivate a coercive struggle of de facto power preferred by autocrats.[80]

Although the 2020 election occurred outside the period of my study, it clearly continued the application of disinformation as a divisive weapon which eventually lead violence at the Capitol on January 6, 2021. Political violence is a predicted and predictable result of disinformation as applied by Russia or those who adopt Russian tactics. In all these ways, Italy and the United States conformed with expectations. However, the United States Government did also act unexpectedly in some other ways.

The United States response to Russian disinformation varied from my predictions in two main ways. First, although the government was handicapped from 2016-2020 by a

77. Christiani, 2020 and Bechis, 2020.
78. Economist Intelligence Unit Democracy Index 2020, p. 9.
79. Benkler, 2020.
80. Acemoglu and Robinson, 2006.

chief executive who actively obstructed full reckoning with the most damaging Russian influence operation of the period, still the government took strong actions against Russia. For example, President Obama with Congress created the Global Engagement Center in 2016 to combat not only Islamic State but also Russian propaganda.[81] And multiple investigations by Congressional committees, intelligence agencies, and law enforcement all resulted in a consensus view that Russia had attacked United States elections.[82] This resulted in arrests, indictments of Russian individuals and organizations, and new sanctions against Russia agreed to by a veto-proof majority of Senators even while the body was Republican controlled.[83] Despite the President's protest, the government still found ways to respond directly to the threat. And, just as the United States Government was not completely dissuaded by the President's lies and subversion, the United States Government, neither was it focused solely on domestic responses. Following the disastrous 2016 attack and lack of public acknowledgement from Republican leaders that Russia had interfered in the election, the United States Government remained engaged abroad to help allies avoid similar worst-case outcomes in their elections. American intelligence, for example, was helpful in blunting Russian interference in the 2017 French Presidential election. The National Security Agency established and shared with France attribution that tied Russian actors to election attacks, enabling the Macron campaign's effective response.[84] The United States changed over this period and acted. The actions were late and weaker than they likely would have been had they been headed by a

81. Stengel, 2019.
82. Applebaum, 2021 and Davis, 2018.
83. Jopling, 2018.
84. Nance and Reiner, 2018, and Jopling, 2018.

President who placed United States interests above his own, but the actions were still significant and not just in the United States.

Overall, the high capability low will states' responses repeated a theme from the low capability low will states that there is a temporal quality to state action combatting disinformation. A state's response to similar types of disinformation can vary over relatively short periods. Before the 2016 election in the United States, for example, disinformation was one issue among many in a noisy democracy which mainly expected a continuation of Obama administration policies under the first female president. Instead, the issue instantly moved to the top of many policy agendas and parts of the government pursued it even as the President did not. And even in Italy, the government officially acknowledged publicly by 2020 that Russia and China were spreading disinformation in Italy to undermine democracy.[85] This leaves open the question moving forward of who will control policy. If actors like Donald Trump, Matteo Salvini, or other purveyors of disinformation regain power in the United States and Italy, democracy will continue to backslide. If actors who support democracy at home and abroad are chosen to lead, perhaps the lessons learned from 2013-2020 can inform actions taken to rebuild damage done to institutions.

85. Christiani, 2020 and Bechis, 2020.

High Will, Low Capability: Australia, Finland, Lithuania, Netherlands, Sweden

Coorelates of War CINC			NCPI Ranking (Information Control and Norms)			OECD Trust		
	Avg. 2013-16	Since 1991	State	Average		State	Average	
United States	0.13204	Q1	United States	1.0	Q1	Netherlands	61.31	Q1
Russia	0.03786	Max .15630	United Kingdom	7.0		Germany	58.83	Max 80.86
Germany	0.01688	Q2 .01998	Russia	7.5		Canada	58.02	
United Kingdom	0.01433		France	10.0	Q2 9.4	Finland	57.01	
France	0.01374		Australia	11.0		Sweden	55.48	Q2 55.73
Italy	0.01150		Sweden	11.0		Russia	51.57	
Canada	0.00861	Median .01040	Canada	12.5		Australia	45.66	
Spain	0.00764	(Q3 .02281)	Netherlands	14.0	Q3 12.8	United Kingdom	40.42	Q3 44.92
Australia	0.00674		Germany	15.5		France	36.22	
Poland	0.00549		Spain	17.5	Q4 16.0	United States	35.09	
Netherlands	0.00398	Q4 .00543	Lithuania	22.5		Lithuania	33.86	Q4 34.52
Sweden	0.00210	min .00039	Italy	24.0		Poland	33.11	Min 14.57
Finland	0.00151					Spain	29.10	
Lithuania	0.00041					Italy	25.19	

Table 7: Ratings for High Will, Low Capability States

			Expected Action	
Legend:	High Will	Low Capability	State employs indirect (defensive) efforts. Ex: defense alliances, multinational institutions, public education	Australia Finland Lithuania Netherlands Sweden
Observed			Protect democratic institutions/processes domestically	Australia Finland Lithuania Netherlands Sweden
Inconsistent			Build resiliency domestically	Australia Finland Lithuania Netherlands Sweden
Not observed			Integration among domestic sectors: government, media, society	Australia Finland Lithuania Netherlands Sweden

Table 8: Overall Findings for High Will, Low Capability States

Because large states garner outsize attention in international media and global politics, I had little familiarity with many aspects of the responses by the high will low capability states highlighted in Table 7. As such, I found this group most interesting to research. As outlined in Table 8, my theory predicts that because the Russian threat to them comes from a relatively more powerful adversary and because this is more likely to be perceived earlier and taken more seriously, these states would be effective as laboratories for developing creative ways to push back against Russian disinformation. Overall, evidence supported those predictions.

The high will low capability states in my sample are Australia, Finland, Lithuania, Netherlands, and Sweden. All of them are below average in the aggregate CINC measure. In fact, these states include the lowest four and five of the lowest six average CINC

scores from 2013-2016. Their small size, then, does seem correlated to taking the Russian threat more seriously than the more powerful states in the sample. These states are also mostly middle of the pack for Belfer NCPI rankings of Information Control and Norms. Australia, Sweden, and the Netherlands are all clustered around the mean. Lithuania was far down the list, only above Italy. Unfortunately, the Belfer NCPI rating did not consider Finland. But I assume that Finland would score close to Sweden since the two are so similar in their other measurable scores, in their approaches, and in their geography, history, and longstanding suspicion of Russia. These states do vary in their Organization for Economic Cooperation and Development Trust rankings but made up four of the top six scores among the sample. Lithuania is an outlier here, scoring in the bottom quartile. I believe in the case of Lithuania, high will to resist Russian disinformation is consistent with low trust in government; Lithuania is a former Soviet Republic bordering Russia. It is a new democracy with a long history of Soviet control and Russian influence so it is understanding that its people could both distrust its government and maintain alertness to Russian interference.

Of the four groups of states in my sample, the high will, low capability grouping most closely conformed to expectations in that these states employed defensive efforts, acted to protect democratic institutions domestically, emphasized building resiliency domestically, and integrated responses among domestic sectors.

First, these states employed indirect or defensive efforts. Being too small to confront Russia head-on, I predicted that these states would employ responses like prioritizing defense alliances, multinational institutions, public education campaigns, and total

defense doctrines. From 2013 to 2020, many of these states already had or updated "total defense" doctrines which put responsibilities on all citizens to resist Russian disinformation— in regular day to day life, but also as part of resisting any period of crisis, such as an invasion by, or conflict with Russia. The doctrines are not only part of the National Security community, as some of these states publish handbooks to every household detailing why Russia is a threat, what to do about it, and how to resist in the case of an invasion.[86] This shows the degree to which these states assess Russian information operations.

Further, when I was thinking through my theory, my conceptualization of defense alliances and multinational organization really included just NATO and the European Union. However, these states are involved in supporting not only each of those, but also layers of multinational efforts of which I was previously unaware. Sweden, Finland, and Lithuania, for example, cooperate with each other and several other states in the Nordic-Baltic 8 defense framework.[87] The mix of states in that framework include NATO members and states which have decided against NATO membership— largely because of the Russian threat— but highlights the strategy of cooperating to balance against a large external foe.

Second, the high will low capability states acted to protect democratic institutions and processes domestically. The Netherlands provided a particularly clear example. Although there were significant changes to laws protecting democratic processes, particularly surrounding elections and freedom of expression issues, the Netherlands methodically

86. Hanzelka and Pavlikova, 2021, and Flanagan et al., 2019.
87. Flanagan et al., 2019.

and publicly underscored its commitment to rule of law. Famously, a Russian-made missile in 2014 brought down a commercial airliner over Ukraine killing all aboard including nearly 200 Dutch citizens.[88] The Russian Government immediately began employing disinformation about the incident as part of its invasion of Ukraine. The Dutch Government, however, launched through its Safety Board and investigation to establish the facts, emphasize truth and accountability, and push over time against Russian disinformation.[89] Through the investigation and follow-on calls for legal accountability, the Dutch Government has through its actions underscored the rule of law and exposed Russian lies regarding the deaths of hundreds of Dutch citizens.

Finally, these states work to build resiliency domestically and to integrate efforts among domestic sectors including government, media, and society. Finland is an example here. The Finnish Government integrates many different leaders and stakeholders in developing its policies regarding media literacy. These include leaders from Ministries of Education and Culture, Justice, Culture and Sport, and others.[90] The government also relies on celebrities and influencers to highlight the threat from disinformation. Because the Finnish government has educated leaders across sectors on the social science underpinning tactics of disinformation, each contributes to pushing back against it.[91] And, the national broadcast network does some reporting in Russian. This not only reaches Russian-speaking Finns, but also achieves influence across the border into Russia.[92] The

88. Higgins, 2017.
89. Golovchenko et al., 2018.
90. Jankowicz, 2018.
91. Ibid.
92. Tiido, 2019.

Finnish approach has been so successful that the Finnish-language version of Sputnik closed because not enough people read it[93].

All the states in this group showed the responses my framework predicted of low capability high will states. The main outlier here was not in how state governments responded, but in how I measured Trust. As mentioned above, Lithuania is an outlier in terms of will. It is clearly a small state and it behaved as a high will state, but its combined lack of disinformation-relevant capabilities and its very low Organization for Economic Cooperation and Development Trust rating could have made it seem as a low will low capability state. In this case, I emphasized not the Organization for Economic Cooperation and Development Trust rating, but the government's statements and actions regarding Russian disinformation. Although its generic will may be low, its will to deal with Russian disinformation specifically is high.

Lithuania clearly views Russia as an existential threat. It has not only taken all the steps I expected of a high will low capability state, but its civil sector has also led the response in some cases organizing informally with other groups, including Ukrainians and actors across Europe, to resist disinformation.[94] I believe that the low trust in government manifested in Lithuania's Organization for Economic Cooperation and Development Trust rating is a combination of hangover from its Soviet history, newness of democratic institutions, and continuous subversion and undermining from Russia. In this case, the Lithuanian Government and its people are attuned to the threat and have a

93. Schia and Gjesvik, 2020.
94. Gerdziunas, 2018, and "Lithuanians Are Using Software to Fight Back against Fake News," 2019.

high will to resist it, but the state is so small and new that its leadership is not so critical as it is in a state like Finland.

Finland and Lithuania are the two smallest states in my sample. They both border Russia, they both understand the threat, and they both have the will to resist. The main difference here is in their histories. During the days of the Soviet Union, Lithuania was subsumed behind the iron curtain whereas Finland was able to stave off full Soviet control through unlikely victories in multiple costly wars. Having maintain its independence, the Finnish Government had decades to build trust among its people while the Lithuanian Government had to wait until 1991 before it could operate without central control from Moscow. As a result, Lithuania's history accounts for its low trust, but high will.

In conclusion, this group conformed most to my predictions. The states with limited capability combined with high will were very active in defending against Russian aggression. They employed defensive alliances, total defense doctrines, and public education to protect themselves from Russia. They acted to support democratic institutions and processes, and they built integrated resilient domestic efforts combatting disinformation. These states punch above their weight in showing how to comprehensively address disinformation as a societal threat.

High Will, High Capability: Canada, France, Germany, United Kingdom

Coorelates of War CINC			NCPI Ranking (Information Control and Norms)			OECD Trust		
	Avg. 2013-16	Since 1991	State	Average		State	Average	
United States	0.13204	Q1	United States	1.0	Q1	Netherlands	61.31	Q1
Russia	0.03786	Max .15630	United Kingdom	7.0		Germany	58.83	Max 80.86
Germany	0.01688	Q2 .01998	Russia	7.5		Canada	58.02	
United Kingdom	0.01433		France	10.0	Q2 9.4	Finland	57.01	
France	0.01374		Australia	11.0		Sweden	55.48	Q2 55.73
Italy	0.01150		Sweden	11.0		Russia	51.57	
Canada	0.00861	Median .0104	Canada	12.5		Australia	45.66	
Spain	0.00764	(Q3 .02281)	Netherlands	14.0	Q3 12.8	United Kingdom	40.42	Q3 44.92
Australia	0.00674		Germany	15.5		France	36.22	
Poland	0.00549		Spain	17.5	Q4 16.0	United States	35.09	
Netherlands	0.00398	Q4 .00543	Lithuania	22.5		Lithuania	33.86	Q4 34.52
Sweden	0.00210	min .00039	Italy	24.0		Poland	33.11	Min 14.57
Finland	0.00151					Spain	29.10	
Lithuania	0.00041					Italy	25.19	

Table 9: Ratings for High Will, High Capability States

			Expected Action				
Legend:			Mix of direct (offensive) and indirect (defensive) efforts. Ex: punish attackers, educate population, build and	Canada	France	Germany	UK
Observed	High Will	High Capability	Protect democratic institutions, processes, and norms domestically and internationally	Canada	France	Germany	UK
Inconsistent			Leadership role integrating response to disinformation: domestically and internationally	Canada	France	Germany	UK
Not observed							

Table 10: Overall Findings for High Will, High Capability States

The last, but certainly not least group of states is those with high will and high capability. Cases in my sample include the states highlighted in Table 9: Canada, France, Germany, and the United Kingdom. My framework expects these states will be leaders in the push back against Russia and protecting democracy in their own societies and internationally. Even in rough aggregate measures, the capabilities these states can bring to bear are collectively greater than Russia can muster. When leading in concert with states from other groups, the capabilities of democracies dwarf Russian state power. As described earlier, the main goal of Russian strategy is to pursue its interests aggressively, but just hard enough to undermine its enemies while avoiding triggering a forceful international response. It is these states which will be decisive in succeeding or failing to

secure and promote democracy. These leading states mostly opted for the kinds of responses anticipated by my framing according to will and capability.

According to my conceptual framework, the high will high capability states should have chosen a range of direct and indirect efforts responding to Russian disinformation like punishing attackers, educating domestic populations, and bolstering multinational institutions. They also should have worked to protect democratic institutions, processes, and norms domestically and internationally while taking an active leadership role integrating responses to disinformation at home and abroad. The expected actions are summarized in Table 10.

High will high capability states took a mix of offense and defense against the Russian threat. The United Kingdom provides a good illustration of taking this comprehensive mix of responses. The United States 2016 Presidential election attack was the most successful Russian campaign of the period that I studied. The second biggest blow to democracy was in the United Kingdom's so called Brexit referendum. The attack was part of Russia's same global operation against democracy that targeted the United States election and future European elections.[95] Importantly, the United Kingdom experienced Russian attacks which went beyond electoral interference and included assassinations using poison and nerve agents on British soil. These attacks informed the United Kingdom's adoption of rapid response to Russian operations and disinformation. In 2006, Alexander Litvinenko's murder was a shocking Russian transgression of international norms. When Russian agents subsequently attempted to murder Sergei Skripal and his

95. Nance and Reiner, 2018.

daughter, the United Kingdom Government understood its response needed to be swift and forceful. Within weeks, the newly formed Rapid Reaction Unit (RRU) was formed to take back a fact based narrative and British spies and police gathered enough evidence to expel Russia spies internationally.[96] The United Kingdom Government also moved to a Fusion Doctrine which elevates strategic communications to the same level of national security policy actions as military and financial response options. As such, the RRU is a Cabinet level office and takes two approaches to disinformation: identifying and responding to threats around predictable events like elections and implementing emergency procedures reacting to unanticipated attacks.[97] Both approaches increase the availability of reliable government information that remain visible to the public in an attack, including moving official United Kingdom information to the top of search algorithms which otherwise can get swamped when propagandists flood the zone with disinformation.[98] The United Kingdom in this period showed that it is acting to both defend against disinformation and to take the initiative in prioritizing visibility of reliable information.

France and Canada demonstrated the second expected response for high capability high will states; they integrated responses not only domestically, but also internationally. Any state with high will to fight Russian attacks on democracy should protect its domestic populations from the intended harms. The predicted difference between high and low capability states is how they would behave internationally. Small states will

96. Haynes and Scott, 2021. Episode 1.
97. Levush, 2019.
98. Ibid.

support international efforts, but high capability states should be leaders in protecting democratic norms and institutions. France and Canada led in this period. First, France showed the way forward in fighting Russian disinformation. The French President has consistently sounded warnings about the threat from Russia, employed decoy documents to feed Russian hackers bad information, banned RT and Sputnik from his media pool labeling them "Pro-Kremlin" outlets, hosted the Christchurch conference, and appealed directly to all citizens of Europe to create an European Union democracy protection agency.[99] Additionally, France has used its power to set rules with impacts beyond its borders. French requirements for social media platforms have become de facto European Union standards adopted by large corporations like Facebook and Twitter which have opted to have one standard for operating in many states rather than many state-specific regimes.[100] France has been a vocal, active, and public leader for democracy promotion.

Somewhat surprisingly, Canada has also lead. For the period, Canada adopted significant domestic reforms to protect its elections and raise awareness of Russian influence.[101] Canada also came to lead some international efforts, filling a role which the United States historically could be expected to have filled. With the United States' dysfunction readily apparent from across the shared border, Canada stepped up to fill a leadership vacuum protecting democratic institutions abroad. In stark juxtaposition with President Trump's advocacy to bring Russia back into the G7, Canada built new capabilities like its own Security and Intelligence Threats to Elections (SITE) Task Force,

99. Jopling, 2018.
100. Levush, 2019.
101. Levush, 2019, and Tsurkan, 2020.

and it took the lead in 2018 establishing the G7 Rapid Response Mechanism. Both organizations are efforts integrating domestic and joint international responses protecting democratic processes from increasing threat.[102] The lack of American leadership has even made some strategists in Canada voice the need to consider how the country will act if the United States continues its anti-democratic direction.[103] France and Canada were two leading states integrating responses by democracies to Russian disinformation. The other state in this group did not pursue expected responses as fully as the framework would have predicted.

Germany was an outlier in this group in that its government's responses were least consistent with expectations of a high will high capability state. It was not a consistently strong leader for democratic norms and institutions. Instead, its policies sometimes took both sides of major issues involving Russian attacks on democracy in Europe and globally. For example, before Russia's invasion of Ukraine, Germany was a major proponent of the Ukrainian democratic movement.[104] And after Russia invaded, Germany was a strong advocate for sanctions. But, it has also pursued the Nordstream II pipeline construction which would allow Russia to undermine Ukrainian democracy by circumventing the state, dividing it from Europe, and depriving it of major resources collected through transit fees.[105] Germany has acted strongly to fight disinformation domestically through laws targeting disinformation and hate speech, protecting elections, attributing attacks to Russia, fining outlets that propagate disinformation, and educating

102. Levush, 2019.
103. Homer-Dixon, 2022.
104. Steizenmüller, 2017.
105. Janda, 2018.

its population.[106] However, its focus has been more domestically protective than internationally leading. Perhaps this makes sense given Germany's history, however. It was for decades ground zero for Cold War disinformation and espionage. And, I believe more importantly, there are pockets of significant Russian sympathy in Germany. A confluence of factors— again including American dysfunction and unreliability— its population likely account for its pragmatism in dealing with Russia.[107] Germany's response was not as comprehensive or internationally oriented as predicted for a high capability high will power, especially for one of two major leading states of the European Union.

In conclusion, most of the high will high capability states responded as predicted to Russian disinformation. They employed a mix of state responses aimed at defending themselves while also working to advance democratic norms and institutions within their own systems and internationally. The responses they took from 2013-2020 will be relevant for the foreseeable future. Events since 2020 have only underscored the importance of pushing back against disinformation. Since then, the threat has only metastasized.

Conclusion

Having considered each group of states according to their will and capability ratings, there are two lessons that emerge from their reactions: will is more important than capability, and individual states' responses are not as static throughout the period as I expected.

106. Hanzelka and Pavlikova, 2021, and Levush, 2019.
107. Wood, 2020.

In the end, will seems to be more the more important driver. As evidence, the group which most conformed to my theory was the high will and low capability grouping. These states were very active resisting Kremlin disinformation. Their relative lack of capability compared with Russia, small populations and militaries, social cohesion, and mixed histories with Soviet propaganda all resulted in comprehensive policy approaches. These states, though limited in resources, found creative ways to maximize those capabilities to fight disinformation more effectively than some high capability states. Their will generated integrated action at all levels within society— emphasizing responsibility even to the individual level— and with neighbors and allies. Further, states that had low will struggled to find consistent, effective policies whether they were low or high capability. Even the most capable state in the sample, the United States, was schizophrenic throughout the period. Some elements including the Congress, and, at times, various Executive agencies took strong actions to punish Russian propagandists. However, the response was hamstrung by a sitting President who did not fully organize the United States response. The United States' capability, then, was still deployed to push back against Russian attacks but could have been much more effective with a leader who chose to generate will instead of undermining will.

This recalls the second lesson: many of the states' approaches morphed throughout 2013-2020. My going in assumption was that the low will low capability states would be unlikely to take any action at all. Like a fighter who has been knocked out, these democracies lack the capability or will to resist. So, it was surprising to see that if external meddling is perceived as having gone too far, even low will states can quickly

turn to addressing the threat. In the period, low will states like Spain and Italy began to stir to get off the mat. That indicates reason to hope that the other low will states— Poland and the United States— can similarly wake up to the threat before backsliding any further than they already have.

In the next chapters, I will consider two states in greater depth: the United States and Finland. In many ways, these states are opposites in will, capability, and outcomes dealing with Kremlin information attacks since 2013.

CHAPTER 4
FINLAND: HIGH WILL, LOW CAPABILITY

"The term itself may indeed be new but the concept is as old as warfare and diplomacy, and Russia's neighbors have had to live with it for a long time. Few countries can match Finland's long experience of dealing with Soviet and Russian hybrid warfare —before, during, and after the Cold War—and few countries have had as much success in standing up to it."

-René Nyberg, former Finnish ambassador to Russia, on Russian Hybrid Operations[108]

Introduction

If one designed a state to provide a counterpoint example to the United States, in many ways, that state would resemble Finland. While the United States is a large, diverse, global power separated by an ocean from Russia, Finland is not. It is a small, homogeneous nation with a long history of struggling with Russia, the much larger state with whom they share an 830-mile border.[109]

Given these differences from the United States, we might also expect a different approach to Russian disinformation campaigns. This chapter investigates whether that was the case. In Chapter 3, I argued that Finland was a high will low capability state, which implies that it should respond to the Russian disinformation campaign in four main ways: by employing defensive efforts like alliances and public education campaigns, by protecting democratic institutions and processes domestically, by building domestic resiliency, and by coordinating integrated responses that include several sectors of society.

108. Nyberg, 2018.
109. Standish, 2017, p. 7. "But Finland does have one thing that drives the Kremlin to distraction: an 830-mile border with Russia. Fears over NATO's eastward expansion — including, potentially, to Finland — are behind much of Russia's aggressive posture toward the West."

Overall, I find, consistent with my argument, that Finland's response included all those expectations of a high will and low capability state. The Finnish Government coordinates with a wide range of government and civil society actors to combat disinformation.

Coordination on disinformation is only one aspect of a much broader Finnish response; the government prizes a long-term resilience strategy, as outlined in its Yhteiskunnan Turvallisuusstrategia (Security Strategy for Society).[110] This strategy embodies a security approach that Finland has practiced at least since the early Cold War. In managing a long history with Russia and the Soviet Union, Finland has had to balance its ties to Europe and the United States as a small state of the West with its security imperative to avoid provoking overt aggression from its immediate existential threat next door in Moscow.[111] This has led to a policy of partnering with, but never joining, NATO. The Security Strategy for Society's balance is temporal; it includes measures for short term emergencies, but its real purpose is recovery and long-term social stability.[112]

This policy approach is how Finland has achieved success against Russian disinformation. Over decades, the Finnish Government has prioritized building a stable society built on education, capable governance, and shared responsibility of leaders and

110. "Security Strategy for Society – Turvallisuuskomitea", 2017, p. 7. "The fact that the comprehensive security model applied in Finland covers all levels and actors of society is its strength…In this model, all actors taking part in coordinated security work or security activities closely supporting it are security actors. Individual citizens also play an important role in independent preparedness and in enhancing the resilience of Finnish society."
111. Szymański, 2018, p. 32. "Finland assumes that as a country situated in the periphery of its civilisational base (the West) and bordering on a potentially hostile power, it must constantly demonstrate its will and readiness to defend its sovereignty."
112. "Security Strategy for Society – Turvallisuuskomitea", 2017, p. 22. "Trust is built during normal conditions. The authorities must observe the same fundamental principles and values in normal conditions, during incidents and in emergencies so that they can retain the trust of the citizens."

citizens.[113] This strategy has paid off in the highest single-year Organization for Economic Cooperation and Development trust rating among all countries in the cross-national survey sample.

This approach has also yielded a firm but flexible posture regarding threats from a diminished but adapting Moscow.[114] Such threats have included disinformation launched from Moscow during the Cold War and now from Russia during a major resurgence early in the 21st Century.

This chapter and the United States case study will follow a similar structure to test my theoretical framework. First, each case study will begin by placing Russian attacks in their country specific context. Understanding the attacks in each state helped explain the degree to which each state displayed will and capability to respond effectively. Second, the case studies analyze what unique characteristics resulted in the state's will and capability categorization. Third, I assessed how closely the states' responses conformed with predicted responses internationally and domestically. Finally, each case study discusses lessons learned for my framework and concludes with a discussion of what the findings may mean for the states in the future.

Background and Context of Disinformation in Finland

Russian disinformation in Finland is nothing new: for decades, the Soviet Union had active disinformation campaigns in Finland, and recent Russian efforts need to be seen

113. Bjola and Papadakis, 2020, p. 658. Finland's education system prioritizes "teaching citizens to identify bias or skewed narratives in their information sphere and to critically engage with new technological platforms like social media."
114. Pynnöniemi, 2019, p. 156. Russia is not as powerful as the United States or the former Soviet Union, leading strategists to a conclusion that the Kremlin, "must respond to emerging threats in a more flexible manner and, if possible, not directly, but with asymmetric measures."

through that historical lens. And the specific applications of Soviet disinformation in Finland have their roots in a long and unique history. That history has not only shaped the intensity of Soviet activity aimed at keeping Finland from fully joining the West, but also in Finland's fierce will to protect its independence from the existential threat of annexation under Soviet or Russian rule.

Finland was part of the Russian Empire since the days of Napoleon, opportunistically declaring independence in 1917 just weeks into the confusion of the Russian Revolution. According to Trotter,

> Seeds of future war had in fact been planted at the moment of Finland's birth. Lenin's government had bitterly resented having to give up Finland so compliantly, but at the time it was done, Lenin was beset by so many other and far more dangerous and immediate threats that he simply had no alternative. The Politburo assumed that propaganda, internal domestic unrest, and a bit of routine subversion would ultimately be enough to bring Finland back into the Communist sphere.[115]

From that moment through the collapse of the Soviet Union, Moscow came close several times to conquering Finland. Finland fought two wars against the Soviet Union during World War II, for instance. The first, or Winter War, started just a month after the German Army invaded Poland. At roughly the same time, the Soviet Union under Stalin attempted to Annex Finland. The Finnish Army lost valuable territory but avoided total defeat in what was a brutal campaign.

During the second campaign within World War II, Finland even fought along with Nazi Germany against the Soviet Union. This is known as the Continuation War and ended only because the Soviet Union, exhausted in 1944 by the wider war, had to

115. Trotter, 1991. page 7.

prioritize resources to fight the Nazis elsewhere.[116] Finland, then, again maintained its independence at a high cost by taking extreme measures to avoid annexation.[117]

Moscow continued influence campaigns throughout the Cold War. The KGB penetrated states and parties throughout Europe, especially in the Baltic region seeking to keep a buffer between the West and Moscow.[118] Specifically in bordering Finland, the Kremlin kept up pressure to keep Finland out of NATO. This ultimately compelled Finland's neutrality, forcing the adoption of Soviet preferences by a nominally independent neighbor. The tactic was even derisively coined "Finlandization," remaining in the Kremlin's lexicon today to belittle their neighbor. The term is offensive to Finns specifically, but also describes Russia's preferred way of dealing with states in its periphery generally.[119]

The technique remains active. The Kremlin aims to compel Ukraine from joining the European Union and it is still pressuring Finland whenever the issue of NATO membership arises. As recently as the month of this dissertation's writing, April 2022, Russia continues its use of threats and military shows of force to compel Finnish neutrality, reportedly having moved heavy military equipment to the border in response to Finland's consideration of joining NATO.[120]

Similarly, the Kremlin also continues its use of propaganda and disinformation

116. Rusi, 2017 and Trotter, 1991.
117. Nyberg, 2018. "Although Finland lost almost fifteen percent of its territory, the country retained its independence. This marked Finland as a unique case among Russia's neighbors. It was the only country that stood up and held its own against the vastly bigger neighbor."
118. Ibid.
119. Lucas et al., 2021. "The ideal relationship for Russia with a neighbor is broadly what it currently enjoys with Belarus, or what in Russian literature is described as 'Finlandization,'" Finns "regard the term… as insulting and inaccurate"
120. Bunyan and Finch, 2022.

targeting Finland. As a Baltic state, and especially as the lone Baltic state directly bordering Russia which successfully maintained its independence from the Soviet Union, Finland is a significant focus of Russian disinformation. Themes of Russian disinformation include a narrative that portrays it as historically part of the Russian empire, who collaborated with Nazi Germany during World War II, and as part of a decadent, declining West bent on bringing social disorder into Russia.[121]

These themes fit into Nimmo's "four Ds" construct introduced in Chapter 2: dismiss, distort, distract, and dismay. The Kremlin's information attacks in Finland highlight the state's history, futility of its security efforts should Russia choose to act against it, and western moral decay. All of this is aimed at "distracting attention from Russian subversion and projecting an impression of indefensibility."[122] The indefensibility narrative tends to portray Finland as a state isolated, peripheral, and marginal within Europe. And while that narrative aims to devalue Finland, the Kremlin also seeks to play up the unity and importance of Finland's Russian speaking population.[123] These themes appeared in several Russian disinformation attacks from 2013-2020 in Finland as discussed in the next section.

Russian Disinformation in Finland

Capabilities and Targets

The Kremlin has pursued its disinformation campaigns in Finland as part of its

121. Lucas et al., 2021.
122. Ibid.
123. Pynnöniemi and Saari, 2017. "specific Russian narratives tailored to the situational context in Finland seeks to portray the country as sidelined within the European Union… Another narrative strives to present the Russian-speaking population in Finland as a united group that is being discriminated against or even threatened."

broader strategic efforts to undermine democracy globally since 2013.[124] Because Finland shares a border and long history with Russia, the range of efforts the Kremlin has pursued is wider than other states more distant from Moscow. Disinformation has been an integrated effort included among other weapons employed in hybrid attacks in Estonia and with outright Russian military invasions into Georgia, and Ukraine. Estonia, for example, experienced in 2007:

> A disinformation blitz claiming falsely… systematic persecution of the Russian minority; A major distributed denial-of-service (DDoS) attack on computer networks. This disabled, briefly, banking and other public services and the mobile phone network, and cut the country off from the global internet making it hard for media outlets and the authorities to get their message across; Kremlin-sponsored youth groups rioting in the streets of Tallinn and besieging the Estonian embassy in Moscow; Economic sanctions on transit and energy supplies; Russian politicians and officials, and those of allied countries, applied intense diplomatic pressure on Estonia, with demands including the dismissal of the prime minister and government.[125]

Georgia and Ukraine experienced many similar activities in addition to military aggression.

Finland has avoided these more extreme mixes of capabilities but is still at risk. As a NATO partner, it does not enjoy Article 5 collective defense guarantee of a full member. Instead, it stays well integrated with Sweden, the European Union, and even more militarily integrated with NATO than some full members. While this has likely contributed to preventing a Kremlin attack using all elements of Russian power, Russia has still employed a mix of capabilities aimed at destabilizing the country since 2013.

The main Kremlin capability employed, as in other attacks globally, was the Internet

---

124. Nimmo et al., 2020 call the global operation "Secondary Infektion." They describe it as "multiple campaigns on social media run by a central entity, which was already active in 2014 and that was still running in early 2020."
125. Lucas et al., 2021.

Research Agency. The paid trolls who targeted Brexit, the 2016 United States election, and many of the other attacks detailed in Appendix A also targeted Finland.[126] The campaign used the Internet Research Agency's mix of trolls and automated bots to amplify its "pro-Putin, pro-Russia, anti-NATO, and anti-governmental" themes along with messages twisting historical narratives and stirring up extreme nationalism.[127]

The targets of these messages are Finland's Russian-speaking minority and Finnish nationalists. These groups are targeted within Finnish society because Russia assesses they are the most likely groups to accept propaganda and because they have demonstrated desire to undermine and disrupt Finland's democracy. Bjola and Papadakis term such groups "counterpublics" which "aim to establish their own counter-knowledge that actively seeks to delegitimise current institutions, on the one hand, and to elevate populist counter-claims to the realm of public debate on the other hand."[128]

The small size does not discount their value in subverting Finnish will. Russian speakers in Finland were only around 1.5 percent of the population in 2018.[129] But, they are growing and present a group that could undermine Finland's high level of unity, trust in government, and Western orientation over time. These counterpublics make great targets for disinformation since they can be "constituted online and empowered by digital platforms, seeking to use themes and topics, often in alignment with the digital propaganda of a foreign government, to undermine or even block the functioning of the

126. See Nimmo et al., 2020.
127. Haynes, 2017.
128. Bjola and Papadakis, 2020, p. 656
129. Tiido, p. 2. "In Finland, the number of Russian speakers has grown steadily since 1991, when it was fewer than 10,000, and in 2018 was approaching 80,000, which constitutes around 1.5% of the total population."

public sphere."[130]

Finally, there are prominent Finnish media outlets and personalities on which the Kremlin relies to spread its narratives. Two large outlets, MV-Lehti and Hommaforum have been equated with filling the same role in Finnish media that outlets like Breitbart plays in the United States.[131] One individual was particularly helpful in spreading disinformation. Johan Bäckman's name appeared repeatedly in multiple attacks over the period. Bäckman, a Finn, was outspoken attacking Finnish journalists and pushing Pro-Russian propaganda during several operations since 2013. The next section will detail how the Kremlin employed its themes and capabilities to pursue its divisive aims targeting Finland.

Attacks Since 2013

The Finnish Government operates with knowledge that the Kremlin continues persistent information warfare with the same strategic goals pursued by the Soviet Union: undermine the Finnish Government and negatively influence the Finnish public to disrupt Finnish relations with the West generally, and with regards to NATO membership specifically.[132]

First, the Kremlin worked to undermine Finland's high trust in its government through information campaigns that blended physical and online elements. As discussed earlier, from Lenin on, Soviet and Russian propaganda has aimed to bring about physical

130. Ibid, p. 657.
131. Bjola and Papadakis, 2020, p. 655.
132. Haynes, 2017. "Finland's Ministry of Foreign Affairs (MFA) identified an advanced persistent threat (APT) in their computer systems that extracted sensitive political and military intelligence over several years." And Szymański, 2018, p. 19 lists Russia's goals as "undermining public confidence in the government, weakening people's pro-European orientation and entrenching the low level of support for NATO membership."

force as an organizational weapon.[133] The Finnish border became a setting for a Kremlin-fueled migrant crisis aimed at making the Finnish government look inept. In fall 2015, Russian border security allowed thousands of undocumented people, including many Afghans who had lived for years in Russia, to cross into Norway and northern Finland.[134] These people were corralled by Russian authorities and criminal smugglers to illegally cross what had been very stable borders for decades.

The Russian government used the physical facts they created on the ground to feed propaganda showing a disorderly border and assigning blame to the Finns. The Finnish government calls such an attack an "information influencing" operation and angrily accused the Kremlin of creating the crisis, offering to help fix it, and then never quite resolving the issue.[135]

The Kremlin picked the timing of the crisis to coincide with European-wide crises of dealing with the flow of refugees out of Syria. The winter of 2015-2016 was an opportunity, then, to concoct a situation of asylum seekers in Finland which could repeat themes playing out in European states everywhere.[136]

In addition to the information influencing at the border, purely disinformation attacks played out online targeting the Finnish government. According to Lucas et al., Russian information attacks continued to push historical grievance and a theme of Finnish

133. Tiido, 2019, p. 5. "As for mobilisation, the most visible events are connected with the remembrance of World War II. In 2018, an "Immortal Regiment" event was organised in Helsinki, at which, according to estimates, between 80 and 200 people took part, beginning with a march through the city centre. The idea… was later taken over by the state for propaganda purposes. The event in Helsinki was well organised, and some of the participants were reportedly brought from outside Finland especially for the occasion."
134. Nyberg, 2018, p. 9.
135. Bjola and Papadakis, 2020, p. 651.
136. See Pynnöniemi and Saari, 2017. "In the winter of 2015–2016, Russia suddenly began to let third country citizens access the Russian-Finnish border to seek asylum in Finland."

duplicity. The Kremlin attacked the Finnish Government as Nazis and war criminals for its actions dating back to the Winter War and the War of Continuation.[137]

While undermining the national government, two Kremlin attacks also focused on the Finnish population itself. One involved children and another targeted a journalist. Regarding children, the Kremlin pushed a highly charged narrative designed to cleave Finnish society internally. Russian media peddled a narrative that Finnish social services were discriminating against Russians Europe-wide by taking away their children, putting them up for adoption, selling them, or handing them to same-sex Western couples. This narrative targets intentionally hyperemotional themes surrounding parents and children, homosexuality, discrimination, and Russophobia.[138] The aim here is reflexive control—to create pressure and division within Finnish society that results in self-disorganization, forcing the government to overreact through strong condemnation. It was meant to distract Finland from taking a strong position against Russia's 2014 invasion into Ukraine.

The other attack specifically targeted free press who had been reporting on the Internet Research Agency. Jessikka Aro, an investigative journalist in Finland, is credited with being the first Western journalist to investigate the troll farm in St. Petersburg. She was severely harassed, doxed, pranked. The attacks on her were led by Johan Bäckman within Finland and propagated mainly on Russian state outlets like Russia Today, Sputnik, and Pravda. Backman held himself up as a human rights activist who was just

137. Lucas et al., page 16. "Russian information attacks have blamed Finland for purported war crimes during its wars with the Soviet Union in 1939-1940 and 1941-1944."
138. Bjola and Papadakis, p 649-50.

working to protect the rights of Finland's Russian minority.[139] Eventually Aro was hounded to the point where she left Finland for personal security concerns.[140] The case resulted in punishment for Bäckman and new laws protecting against the kind of harassment targeted at Aro.

Finally, the Kremlin has consistently worked to spread disinformation to prevent Finland from pursuing full membership in NATO. To accomplish this, Russia uses its information operations to demonize NATO and threaten Finland. To demonize NATO, the Kremlin propagates a narrative that seeks to flip responsibility for aggression in Russia's periphery. In the Baltic region, particularly, Russia claims that it is a victim, not a threat. Rather, it is NATO and the other defense arrangements Finland pursues— like the Nordic Baltic 8 format— which threatens peace.[141] And, the threats to Finland are consistent. Any time the Kremlin perceives Finnish actions or words indicating closeness with NATO, threats ensue to instill fear of military escalation. Russia repeatedly "declares that Finland's NATO membership would result in an adjustment of the Russian military posture to the new situation in the region."[142] These attacks continued throughout the period following Russia's 2014 invasion into Ukraine. Finland has over decades developed multiple capabilities and strategies to blunt the effects of Kremlin propaganda. In the next section, I will outline some of its important actions responding to the Russian attacks.

Finnish Response

139. Bjola and Papadakis, p 650.
140. Lucas et al., 2021 and Tiido, 2019.
141. Lucas et al., 2021.
142. Szymański, 2018, p. 23.

Will and Capability

Given the country's long history of fighting Russian then Soviet then Russian interference in its internal affairs, my framework predicts that Finland will have a high will to resist not only Kremlin disinformation attacks, but all threats from Russia. The threat from Moscow has repeatedly been clear, sustained, and existential. Therefore, the Finnish Government will always view their most serious threat as the much larger state just across the border with which it has already fought multiple costly wars. The government has long budgeted its resources to sustain its society's will deterring, and if necessary, combatting Russian aggression. Given the degree to which Finland has embedded this will in its culture, it is likely to remain high will against all forms of Russian attack, disinformation included, for the foreseeable future.

I recently had the opportunity to talk with a former Prime Minister of Sweden. When the opportunity presented itself, I asked him what the West needs to do confronting Russian disinformation. His response was telling; he appeared exasperated for a moment before outlining that even stronger tactics have been used against Sweden and Finland for decades. Beyond disinformation, Russian influence has historically involved direct meddling within the political parties of Nordic states. Finland and Sweden have been had parallel experiences with Soviet and Russian aggression, but Finland has directly faced all elements of Russian influence.

It made sense, therefore, that in conducting research for the cross-national survey in Chapter 3, Finland was the state which most clearly demonstrated the highest will to resist Russian aggression and malign influence. Finland's shared border and history

alertly guarding its independence from threats emanating out of Moscow have ensured resistance to Russian disinformation has permeated widely throughout all levels of society.

Finland was in the top quartile for average annual Organization for Economic Cooperation and Development Trust ratings among its citizens. Within that high average, however, two trends make its score even more impressive. First, Finland's trust has generally increased from 2012-2020. And second the states measured each year since 2012, Finland had the highest single-year rating of 81% trust in the most recent year measured. Finland has high will to resist Russian disinformation. At the same time, it is a tiny state relative to its powerful neighboring state.

Coorelates of War CINC			NCPI Ranking (Information Control and Norms)			OECD Trust		
	Avg. 2013-16	Since 1991	State	Average		State	Average	
United States	0.13204	Q1	United States	1.0	Q1	Netherlands	61.31	Q1
Russia	0.03786	Max .15630	United Kingdom	7.0		Germany	58.83	Max 80.86
Germany	0.01688	Q2 .01998	Russia	7.5		Canada	58.02	
United Kingdom	0.01433		France	10.0	Q2 9.4	Finland	57.01	
France	0.01374		Australia	11.0		Sweden	55.48	Q2 55.73
Italy	0.01150		Sweden	11.0		Russia	51.57	
Canada	0.00861	Median .01040	Canada	12.5		Australia	45.66	
Spain	0.00764	(Q3 .02281)	Netherlands	14.0	Q3 12.8	United Kingdom	40.42	Q3 44.92
Australia	0.00674		Germany	15.5		France	36.22	
Poland	0.00549		Spain	17.5	Q4 16.0	United States	35.09	
Netherlands	0.00398	Q4 .00543	Lithuania	22.5		Lithuania	33.86	Q4 34.52
Sweden	0.00210	min .00039	Italy	24.0		Poland	33.11	Min 14.57
Finland	0.00151					Spain	29.10	
Lithuania	0.00041					Italy	25.19	

Table 11: Will and Capability Ratings for Finland

Table 11 shows that while Finland ranked among the highest of states over the last decade in Organization for Economic Cooperation and Development Trust rankings, it simultaneously ranked among the lowest ratings for capability. It is the quintessential high will, low capability state. Finland's CINC score ranked second lowest among the cross-national survey sample. And, for the disinformation-relevant scores for cyber power, the Belfer Center NCPI did not even include Finland in their sample, but it is

possible from looking at Finland's actions and other states in the sample to impute how Finland would rank.

If the NCPI had included Finland, it is likely that the Finland would have been somewhere in the middle of the pack. Finland, according to its interest in surviving as a state, has balanced firm defense domestically against Russian influence with keeping a lower, more flexible profile internationally for decades. This is a way to stay sovereign without unnecessarily provoking Russia. As such, I expect that Finland would get high marks for "Information Control" since it has been able to fend off Russian disinformation, but lower marks for "Norms" since it has achieved its information control quietly. This would rank them close to Sweden— which, again, given their similar approach and direct cooperation, is usually a reasonable general comparison.

Some specific Finnish capabilities, though, give it opportunities to prevent the worst effects of Russian disinformation. Two capabilities which long predate disinformation attacks include Finland's long history of self-government and its language.[143] Finland's self-governance has been an antidote to disinformation because the tradition is one of stability and consensus. As such, the government offers ways for minority views to, if not rule, at least have a voice at the table. This provides the opportunity for counterpublics to vent frustrations and participate in the political process without less risk of tearing down the whole system. Integration and assimilation are prized over marginalization and exclusion.

143. Nyberg, 2018. "A high level of trust, both private and public, characterizes Scandinavian societies and is underpinned by a centuries-old tradition of self-government. A small linguistic community is also protected by the effective wall of its language."

If Finnish traditions are democratically inclusive, the Finnish language provides a complementing exclusionary filter. There are only roughly five million Finnish language speakers in the world and unsurprisingly, almost all of them live in Finland.[144] Disinformation is most effective when it penetrates an information environment without making recipients feel like they are being manipulated. Because almost all native Finnish speakers are in Finland, it is hard for trolls to speak authentically into the media ecosystem. Mistakes in grammar, spelling, and syntax that native speakers would not make result in easy queues for inauthentic, even comically so, narratives out of Moscow.[145]

Besides tradition and language, Finnish authorities have invested in several long-term efforts to build capabilities that make the country resilient. Finland has prioritized education, public awareness, and creating a positive national narrative. All of these have contributed to its ability to resist Kremlin disinformation. According to Nyberg, a former Finnish Ambassador to Russia, Finland's emphasis on education has been critical. The society is resilient not because they became alert to disinformation as a threat after Russia's 2013 escalation, but because the government has had a long-term understanding that "Governments must help citizens to become educated, sophisticated, and discerning consumers of information."[146] Resilience cannot be generated in emergencies, it must be cultivated through education in periods of normalcy.

Finland also integrates its resiliency efforts across sectors of society including

144. See "Languages of Finland" by the Institute for the Languages of Finland.
145. Nimmo et al., 2020.
146. Nyberg, 2018.

government, media, intelligence, business, and citizens. While the country's Council for Mass Media focuses on causes and journalistic responses to disinformation, other authorities highlight narratives that the Kremlin repeatedly tries to falsely insert into current events coverage. The overlapping capabilities provide a defense in depth against lies, boost transparency and credibility, eventually yielding Finland's high levels of trust.[147]

Lastly, Finland has invested in training for government officials on combating Russian disinformation by focusing not on what Russia says or does, but on Finland's own dipositive narrative.[148] The President went to the training himself, again underscoring commitment to addressing the problem. Since then, Finland has been communicating effectively, praised for success resisting Russian disinformation, and their trust in government scores have only gone up. This is the result in long term development of capabilities to combat the Kremlin threat.

Finland is a clear case of high will and low capability. It is at the same time one of the least powerful democracies I researched and in possession of sustained high will to fight against Russian disinformation. According to my framework, this means that Finland should demonstrate the four expectations outlined for a high will low capability state in Table 12: it should employ defensive efforts like alliances and public education

147. Bjola and Papadakis, 2020. 649, 59.
148. Standish, 2017, p. 3. "A homogeneous country of 5.4 million people, Finland routinely ranks at the top of the Organisation for Economic Co-operation and Development's quality of life metrics and, in addition to strong social welfare programs, the country's education system is the best in the world, according to the World Economic Forum."

Legend:			State employs indirect (defensive) efforts. Ex: defense alliances, multinational institutions, public education
Observed	High Will	Low Capability	Protect democratic institutions/processes domestically
Inconsistent			Build resiliency domestically
Not observed			Integration among domestic sectors: government, media, society

Table 12: Overall Findings for Finland

campaigns, it should protect democratic institutions and processes domestically, it should build domestic resiliency, and it should coordinate integrated responses that include several sectors of society.

External Expectations: Deterrence and Balancing

Finland has employed defensive measures including bolstering multinational institutions, public education, and defense alliances. As highlighted before, Russian attacks targeting Finland's international ties have included fabricated border incidents and consistent threats over any Finnish decision to join NATO. The Finnish government has chosen a path of delicate balance; on one hand Finland is a full democracy, member of the European Union, and NATO Enhanced Opportunity Partner. It is not only a Western democracy, but also in many ways an exemplary democracy with high marks for delivering what its citizens want. On the other hand, Finland has for decades remained very engaged with Russia, maintaining highly visible military readiness and political connections at the highest levels aimed at reducing the risk of triggering Russia.[149] The

149. Milne, 2022. "Finland is one of the few European countries that did not significantly cut its military strength after the cold war, as its 1,340km border with Russia, and memories of the bitterly fought 1939-40 winter war against the Soviet Union ensured security matters retained a high priority. But Finland has also preserved close diplomatic and commercial ties with Russia."

constant interaction Finland maintains to achieve that balance stems from a clear-eyed assessment of its interests.

Because of its small size, Finland not only balances the West and Russia, but also between defense and engagement with Russia individually. As neighbors, Russian trade provides important opportunity for the Finnish economy. But the threat from Russia is never far from Finnish security policy. Finland knows that it cannot survive fighting Russia alone, but it also assesses that without NATO guarantees, it must maintain a force sufficient to deter another Russian invasion.

So, Finland seeks to deter and balance. Finland avoids Russian inclusion in military supply chains and maintains nearly 300,000 forces in reserve as a deterrent, a relatively large defense force for a country of only five million people.[150] And to balance, it is militarily more integrated with NATO than some full NATO members. It has maintained as close of a relationship with the West as possible while keeping Russia satisfied enough in its neutrality to prevent aggression.[151] Such defensive measures are in line with threat perceptions predicted by my framework.

To combat Russian interference with Finnish NATO membership, Finland has maintained nominal neutrality, but done everything to support NATO short of applying formal membership and Article 5 protection. Finland is a member of the NATO Strategic Communications Center of Excellence. Helsinki is host to the European Centre of

150. Szymański, 2018, p.. 5. "Finland's strategy towards Russia combines economic and political co-operation, intended at reducing the risk of bilateral tensions, with military deterrence. Finland is concerned by Russia's rising military and the Russian vision of the international order based on great powers' spheres of influence in which Finland has to play the role of a buffer zone between Russia and NATO."
151. Pynnöniemi and Saari, 2017.

Excellence for Countering Hybrid Threats, which has been operating since 2017.[152]

Finland has further signaled through personnel assignments its emphasis on the seriousness of its perceived threat from Kremlin disinformation. For example, Finland created a new position of Ambassador for Hybrid Affairs then named an experienced diplomat to the post.[153] This elevates the threat of hybrid conflict through creating the position, then underscoring the seriousness by appointing a prestigious leader to rally international efforts. Bjola and Papdakis (2020) describe the action as one that "contributed to creating a centre of institutional gravity for addressing the issue of disinformation in a more systemic fashion.[154]"

In addition to working directly with NATO, Finland has worked with other partner states in the region in ways designed to move forward deterring Russian aggression in the Baltic. Several NATO members have engaged with Finland bilaterally or through defense alliances such as the Nordic-Baltic 8 format. Though it is not tied through formal agreement directly with NATO, Finland's friends are. And Finland has led specific NATO actions aimed at countering Russian disinformation.

It has also acted against disinformation that Russia employed as a weapon during the Kremlin-manufactured border crisis. At otherwise long-stable Finnish crossing points, Finland responded with updated efforts to seize control of false narratives. In 2016, Finland and Sweden jointly condemned Russian propaganda in the region.[155] And it was after the crisis that Finland sent its officials to Harvard for training on effective

152. Tiido, 2019 and Splidsboel, 2017.
153. See "Mikko Kinnunen Appointed Finland's First Ambassador for Hybrid Affairs," press release from the Finnish Ministry for Foreign Affairs, 2018.
154. Bjola and Papadakis, 2020, p. 659.
155. Pynnöniemi, 2019.

techniques for responding to information attacks. Russia instigated the crisis over Finnish support for sanctions resulting from Russia's 2014 invasion of Ukraine; Finland took the opportunity to confirm support for the sanctions.[156] Finland has shown it will work with anyone who will help push back against Russia: regional neighbors, European Union members, NATO, and the United States. All these measures are in line with defensive measures my framework predicts for a high will state which aims to maximize use of low capability.

Domestic Expectations: Norms, Resilience, Institutions

Finnish authorities have in the recent decade continued to generally emphasize resiliency and protection of their tradition of self-governance. The specific responses to the child custody attacks and the attacks on Jessika Aro demonstrated some innovative approaches and reinforced the value of a resilient society.

As Ambassador Nyberg described, the government has protected domestic institutions to cultivate resiliency at home.[157] The Finnish intelligence service has identified dozens of recent Russian information operations.[158] Most, like the Jesikka Aro campaign and the child custody issue were either initiated, enflamed, or both from Moscow.

The government has taken steps to bolster democratic institutions domestically. In March 2019, the Finnish government passed a law that requests candidates for security postings to prove they do not have dual loyalties to other nations or beliefs that might

156. Ibid.
157. Nyberg, 2018: "The Finnish government has organized courses with Harvard University to train civil servants to recognize a hybrid operation and how to act. The background of the Finnish initiative is the comprehensive security concept built over decades… it emphasizes building awareness and strengthening the resilience of Finnish society."
158. Pynnöniemi, 2019.

undermine national security.[159] This appears to have been in response to concerns raised not only during the cross-border tensions including disinformation operations, but also to recalling previous Soviet infiltration of Finnish politics. Also, responding to the wide-ranging Kremlin efforts to attack democratic elections across Western democracies, prominent national celebrities and officials publicly bolstered the security and reliability of the electoral system leading up to elections in 2019.[160]

In addition to shoring up security positions and elections, the government established new norms responding to information attacks on journalist Jesikka Aro. One of the first new norms advanced by the Hybrid Affairs minister said that harassment "is part of influencing, [trolls/harassers] try to tire individuals so they switch to silence or make journalists write on something else."[161] This is a novel way to link disinformation with criminality. Just as Russian propagandists do not have separate conceptions of physical and information domains in political warfare, this Finnish approach treats disinformation attacking journalists as a weapon against democracy since self-censorship degrades the range of participants who engage in the public sphere.

Finnish law has also reframed the problematic debate of bad faith actors who exploit freedom of speech protections to harm democracy. Finland has developed a concept of freedom of communication through a new principle: "viestintärauha. Though there is no exact English equivalent, it approximately translates to 'communication peace,' which can be interpreted in this context as freedom from unsolicited communication."[162]

159. Tiido, 2019.
160. Schia and Gjesvik, 2020.
161. Quoted in Bjola and Papadakis, 2020, p. 653.
162. Bjola and Papadakis, 2020, p. 654.

The leading Finnish propagandists attacking Aro were convicted of defamation and stalking. Their sentence was made more significant because their motivation was to undermine a journalist doing work critical of Russia.[163] Finland's long-term commitment to domestic resilience also informed the government's reaction to the Russian child custody attacks. All these steps indicate that, in accordance with my framework, the high will Finnish Government acted to protect democratic norms and institutions domestically while building a resilient society.

Finland also demonstrated the final expectation pursuing a comprehensive response to disinformation that integrates many different leaders and stakeholders. This showed in its policies regarding media literacy which were developed by leaders from Ministries of Education and Culture, Justice, Culture and Sport, and others.[164] Because the Finnish government has educated leaders across sectors on the social science underpinning tactics of disinformation, each contributes to pushing back against it.[165]

These education campaigns have included not just training for government officials, but the public and especially children. Since the 1960s Finland has recognized the security implications of Soviet, now Russian, propaganda and has emphasized media and information literacy as a "civic competence."[166] The government has supported this goal in school curricula and in media campaigns. Critical reading of the news is taught in

163. Ibid: "In a landmark decision, the Helsinki District Court found in October 2018 that Mr. Janitskin and Mr. Backman had worked together to slander Ms. Aro and had committed "an exceptionally aggravated set of crimes" because their primary motive was to undermine her work investigating "Russian information threats" by destroying her "professional credibility and reputation as a journalist specializing in Russian affairs."
164. Jannkowicz, 2018.
165. Ibid.
166. Ibid.

schools.[167] This strategy of education, along with cultivating trust in the government, prevented highly emotional and Kremlin-scripted disinformation from gaining traction during the child custody attack.

The integrated response during the child custody attack included the ministry most directly targeted— the Ministry for Social Affairs and Health. Since a framework for coordinating responses across the government already existed, Social Affairs and Health had open lines of communications to other critical Finnish actors in Foreign Affairs and embassies. Further, the trust established with including media organizations in the effort facilitated "debunking child-custody disinformation almost in real-time.[168]"

Further, this campaign highlights another effect of Finland's strategic engagement with Russia. Finnish elites can translate outreach to Russia to bolster credibility with Russian-speaking Finns.[169] As a result of some combination of a resilient public and trust in government credibility, the child custody attack failed. Not even the targeted Russian speaking Finnish counterpublic accepted the narrative. [170]

That dynamic has also been evident more widely. The collective understanding that Russian disinformation is a threat impacts media coverage of other Russian themes. Main Finnish outlets were critical of Russian narratives leading up to their 2014 invasion of Ukraine, for instance, in ways that contrasted with media in other countries which have

167. Haciyakupoglu, et al., 2018.
168. Bjola and Papadakis, 2020, p. 650.
169. Szymański, 2018, p. 5. "Finnish decision-makers also capitalise on diplomatic contacts with Russia in domestic policy: as an opportunity to demonstrate to the electorate their pragmatic attitude in relations with a country which is viewed in Finland as a great power."
170. Ibid. "Despite the intense promotion of the Russian media, the 'child custody' campaign has failed to become an identity defining issue for the Finnish counterpublic."

journalistic norms that help propaganda to spread.[171] In fact, the Kremlin even closed the Finnish-language version of Sputnik closed because not enough people read it.[172]

Even better from a Finnish perspective, Finnish credibility extends into Russia. For example, the Finnish national broadcast network does reporting in Russian. This not only reaches Russian-speaking Finns, but also achieves influence across the border across the border.[173] Finland's government has employed effective strategies generally against Russian disinformation and specifically in the cases regarding operations targeting Jesikka Aro and child custody. By bolstering its institutions and inculcating resiliency among its people, Finland has shown how Kremlin disinformation can be disrupted. This integrated, resilient response accords with expectations of my framework.

Lessons Learned

As a case study on how to deal with Russian disinformation, Finland is a clear example of a high will low capability state. Its response was in line with predictions from my framework. It employed defensive efforts like alliances and public education campaigns. Finland protected its democratic institutions and processes domestically and built domestic resiliency. It also clearly coordinates integrated responses involving a wide range of actors across society. The context of Finland, specifically, offers three main lessons for the framework: disinformation should not be considered in isolation, Finland's efforts building resiliency predate the 2013 escalation, and context matters: what works in Finland may be impossible to repeat fully in other states.

171. Pynnöniemi, 2019
172. Nyberg, 2018, Jopling, 2018, and Schia and Gjesvik, 2020.
173. Tiido, 2019.

First, Russian attacks on Finland show that disinformation cannot be considered in isolation. In developing my framework, I considered disinformation operations as a Russian line of effort this is incomplete. Russia employs disinformation as part of "wider influence operations that use political, economic, legal, and other tools to exacerbate ethnic, cultural, demographic, diplomatic, linguistic, regional, and other divisions."[174]

Focusing only on disinformation will misinterpret the broader application of Russian malign influence as it situationally combines different elements of its state power. And disinformation must also be considered in recent historical attacks. The Russian generated crisis at the border with illustrates these points. Russia did not just tell lies about how inept the Finnish government was. Rather, the Kremlin mixed the lies with public actions, bringing Afghan refugees to a border crossing at a time when all of Europe was dealing with a flood of Syrian refugees. The crisis involved real victims and exploitation, real racism and xenophobia and aimed at provoking a real overreaction in Finland to feeding what Bjola and Papadakis (2020) have termed "information impulses."[175]

The physical actions and the disinformation each complemented the other, so states should be prepared to have options that include physical responses. The disinformation campaign repeated patterns seen previously at the Norwegian border, then again in 2021 at the Polish border with Belarus. Understanding the repetitive nature of Russian operations makes the false narratives less likely to gain wide acceptance in target

174. Lucas et al., 2021.
175. Bjola and Papadakis, 2020, p. 652. "Events like this can be seen as 'information impulses' because rather than being disinformation as such, they combine disinformation with public actions. Put simply, this event was more than a traditional threat from a larger country to a small country"

populations and it should provide opportunities for better coordination of physical responses by border guards, nongovernmental organizations, and communicators.

Second, Finland has found a way to resist Russian disinformation, but their approach had been established long before 2013. The Russian threat in Finland is real, pervasive, and existential. Therefore, Finland has invested for decades in two things: shoring up resilience at home and emphasizing cooperation abroad.[176] The Finnish approach balancing NATO and Russia is central to this approach. Finland maintains what it believes necessary to deter an attack, but hedges by engaging widely with NATO, the European Union, the United States, and other states around the Baltic Sea to make sure it has layers of integration internationally. This balance over time has shaped Finland's investments in society-wide readiness, which, as Pynnöniemi and Saari describe:

> means increasing society's crisis tolerance and resilience, ensuring the readiness and ability to act of the political and administrative leadership of the country, updating legislation, and investing in defence and intelligence. The Finnish tradition of comprehensive "societal security" offers an excellent basis for national cooperation on hybrid influence between various actors: government, local governments, civil society, and business actors.[177]

The traditions that yield societal security include characteristics which decrease the spread of intentionally destructive disinformation. One final indicator of Finnish resistance to consider: since the Russian invasion 2014 into Ukraine, Finnish public opinion regarding Moscow has become more negative, but because the public has such trust in its government, Moscow remained low among a prioritized list of worries even

176. Pynnöniemi and Saari, 2017.
177. Ibid.

four years after the attack.[178] This means that my framework should account not just for a country's will, but the dynamic nature of will over time. A consistently high will state will react differently when attacked than a state which is in a period of heightened or lessened will.

Finally, the third lesson from this Finland case study is that what works in Finland may be impossible to repeat fully in other states. Ambassador Nyberg argued that for better or worse, the Finnish will to resist Russian aggression is born of its sustained fight for survival. That fight has deeply ingrained resilience in Finnish culture.[179] And Jed Willard, the director at Harvard who trained Finnish officials on narrative control has also said that the state is an outlier with a small homogenous population, high standard of living, strong social welfare, and world class education system. This, combined with the government's appreciate that disinformation is "as real as war" has allowed the government to provide comprehensive leadership that its people reward with trust enough to follow.[180] This is a rare combination and tough to replicate. It will put Finland in good position to deal with future attacks that are sure to come. This means that other states in the high will low capability group would likely each have unique elements which contribute to their own will to resist disinformation.

178. Szymański, 2018, p. 23. "The Russian threat has such a distant place in the poll on the one hand because this topic is on the margins of public debate and, on the other because Finns are used to the neighbourhood with Russia and trust their public institutions, in particular, the army (this level of trust is the highest in the EU)."
179. Nyberg, 2018. "Whether one considers Finland lucky because resilience came naturally to its citizenry as a matter of national survival, or unlucky because it did not have that choice, its example demonstrates that resilience is not something that a nation can acquire in a short period of time."
180. Standish, 2017, p. 3. "'This stuff is real. It is as real as war,' said Willard. 'But the Finns very quickly realized this and got out in front of the problem.'"

Future Challenges

Moving into the future, factors will change that have for decades driven of Finnish security strategy, which will impact how it responds to disinformation. Finland is still likely to remain focused on building domestic resilience but will have to adapt to changing technology. And, given Russia's 2022 further invasion into Ukraine, Finland is increasingly likely to become a full member of NATO, risking Russian escalation in response.

Domestically, some of the historical protections which have favored Finland's ability to resist Kremlin disinformation will weaken, requiring an adaptive focus sustaining societal resilience. For example, the Finnish language as an effective screen against non-native speakers will become less effective. Already, digital applications are much more effective in translating messages to any number of languages. It is right now possible for English speakers to interact now with Russian or Ukrainian language tweets coming out of the war zone.[181] In short order the translations will become more accurate, enabling disinformation to penetrate filters that used to prevent its spread.

Also, despite its success defending against disinformation at the societal level, Finns are still human; there will always be a risk of being undermined by day-to-day disinformation as it continues to be targeted at lower and lower levels over time.[182] If enough individuals start forming an effective counterpublic, as the Russian speaking

181. Swisher, 2022. Interviewed Clint Watts, who said that language is not the barrier it used to be. For example, it is possible for non-Russian speaking Twitter users to engage with Russian content during the war in Ukraine by having real-time translation.

182. Bjola and Papadakis, 2020, p. 638. Finland's overall societal resilience has come from institutions enacting "transparent and proactive policies grounded in collaboration and research. However, these efforts are at risk of being weakened by the rise of influential counterpublics unless" Finland can prevent disinformation from spreading at the individual citizen level.

population has thus far not formed, Finland remains susceptible to harm. The Finnish will to resist remains an example, however, and is deeply felt in its culture. The struggle to maintain that independence will continue indefinitely.

Internationally, the 2022 Russian escalation in Ukraine has the potential to fundamentally alter Finland's decades old security strategy. Finland has been formally neutral in the struggle between Moscow and the United States. For fear of provoking Russia, Finland has balanced engagement and participation with both powers, never wanting to be perceived as fully aligned either way. Finland was a proponent of sanctions for Russia's 2014 invasion and annexation of Crimea. The resulting balance between "NATO and Russia has created an arena for both NATO and Russia to continue fighting for influence inside the country."[183] This is sometimes seen as weakness, derisively mocked as "Finlandization" in Russia, but has at times given Finland leverage. Finland used its neutrality and interactions with NATO strategically to advance its own national security goals, not to expedite membership.[184] In recent years, though, the influence operations out of Moscow coupled with military aggression may alter Finland's decision to stay neutral.

As Ambassador Nyberg stated, "The border incidents exploited the Finnish population's anxiety over the growing number of refugees. It backfired and has not been forgotten. The April 2016 report on The Effects of Finland's Possible NATO Membership, commissioned by the Finnish Ministry of Foreign Affairs, noted 'Russia's propensity to create a problem, then leverage it and offer to manage it without necessarily

183. Haynes, 2017.
184. Ibid.

solving it.'"[185] And, even while Russia is fighting in Ukraine, the Kremlin makes sure to signal threats to Finland over joining NATO.[186] The threats against NATO are the same ones Russia made against Ukraine. Had Ukraine been a member of NATO, it is unlikely Putin would have invaded and Finland sees that recklessness as an existential threat.

Finally, the engagement that Finland has pursued with Moscow increasingly comes with security risk.[187] It remains to be seen how isolated Russia will be from the United States and European Union because of recent sanctions, but even before the sanctions economic relations with Russia was a risk. The trade between Finland and Russia, particularly of energy supplies, is problematic since energy is one of the complementary elements of power the Kremlin weaponizes in conjunction with disinformation. Again, the critical thinking of Finland's population is taking on new information and changing opinion. This time, the mix of Kremlin information attacks on Finland, its manufacturing of a border crisis, and its further invasion of Ukraine have Finns discussing NATO membership with renewed seriousness. Before this crisis, support for joining NATO occasionally reached 20 percent support among Finns. After the invasion, that increased to over fifty percent and two months into the war support polled at 68 percent.[188] Finland has not survived Russian influence and aggression for this long to risk being the next Ukraine. The last decade of Kremlin disinformation as part of a suite of aggressive actions taken against its neighbors may backfire, making Russia look out of control,

185. Nyberg, 2018.
186. Bunyan and Finch, 2022.
187. Pynnöniemi and Saari, 2017 "To cope with problems stemming from Russia's geoeconomic 'actorness', policymakers need to be more aware of Russia's inner logic in Finland and elsewhere… Russia does not hide its geoeconomic logic of action in its external and internal energy policies."
188. Langfitt, 2022.

reckless, and desperate. This appears to be driving Finland closer to full NATO membership.

CHAPTER 5
UNITED STATES: LOW WILL, HIGH CAPABILITY

"Following attacks like Pearl Harbor and 9/11, United States presidents have rallied the country and the world to address the challenges facing the nation. Yet the current President of the United States has barely acknowledged the threat posed by Mr. Putin's repeated attacks on democratic governments and institutions, let alone exercised the kind of leadership history has shown is necessary to effectively counter this kind of aggression. Never before in American history has so clear a threat to national security been so clearly ignored by a United States president. The threat posed by Mr. Putin's meddling existed before the current United States Administration and may well extend beyond it. Yet, as this report will demonstrate, the Russian government's malign influence operations can be deterred."

From "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for United States National Security", 2018, p. v.[189]

Introduction

Having just considered Finland in the previous chapter, it is useful to study a very different case: the United States. In contrast to Finland, the United States is a much more powerful state—the world's lone superpower—with greater information capabilities, but it lacks Finland's unity and will (as well as a border with Russia). Given these differences, we might also expect a different approach to Russian disinformation campaigns. This chapter investigates whether that was the case.

In Chapter 3, I argued that the United States is a low will high capability state, which implies that it should respond to Russian disinformation campaign with a weakened state reaction, use of disinformation against domestic audiences, democratic backsliding, and deepening domestic division.

Overall, I find that my framework predicted some, but not all, of the United States government's responses. The most successful attack during the Kremlin's global

189. "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for United States National Security", 2018, p. v.

disinformation operation was the 2016 attack on the United States Presidential election. The United States did little in response during the attack and the winner of the 2016 election, Donald Trump, himself spread significant amounts of dis- and misinformation.[190] However, the United States Congress— and many executive branch agencies— did pursue vigorous responses after the election attack that aimed not only at addressing Russian disinformation domestically, but also helping other democracies develop their defenses. This tension—between the government's countermeasures and Trump's refusal to condemn Russian disinformation—highlights the inconsistency of the United States response.

The United States was consistent with my framework's other expectations of a low will high capability state. It did suffer continuing institutional weakening and degraded individual rights after Russia's campaign to subvert democracy. After being reformed in the image of President Trump, one of the two major American parties has become less committed to democracy embracing election disinformation and loyalty tests as tools for maintaining power domestically.[191] Relying on a partisan feedback loop that includes an activist media ecosystem and elected officials[192] the Republican party has employed disinformation to undermine confidence in free and fair elections, advocate and use violence against peaceful protests, and abandoned many norms that undergird

190. Senator Ben Cardin writing in "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for United States National Security", 2018, p. v. It "must be noted that without leadership from the President, any attempt to marshal such a response will be inherently weakened at the outset."
191. Bennett and Livingston, 2018, p. 126–127. Declining public confidence in democratic institutions undermines the credibility of official information in the news and thus opens publics to alternative information sources.
192. Benkler et al., 2018, p. 8. The right-wing media sphere has been so closed that it makes the United States public discussion "vulnerable to disinformation, propaganda, and just sheer bullshit"

democracy.[193] The weakening of the institution, then, correspondingly weakens individual rights. This chapter outlines how these impacts at once show the ineffective response to, and the cumulative damage from, a serious threat posed by Russian disinformation. My framework anticipates this reaction from a low will high capability state.

Background and Context of Disinformation in the United States

As highlighted throughout this work, Russian disinformation adapted Soviet disinformation techniques for a changed context. The United States and the Soviet Union fought for influence globally for decades, including using disinformation. The United States eventually abandoned disinformation campaigns, as these inherently undercut its values and interests.[194] The Soviet Union, however, continued to develop anti-democratic disinformation tactics and techniques until its collapse.[195]

Since the end of the Cold War, there has been an important change in the United States' media environment that make it uniquely easy to exploit using updated information technology. According to Humprecht et al., the United States media is "low-trust, politicized, and fragmented,"[196] making it the most vulnerable worldwide to online disinformation:

> The country stands out because of its large advertising market, its weak public service media, and its comparatively fragmented news consumption. The enormous size of its market—and its competitive and commercial culture—makes the United States attractive for producers of disinformation targeting social media users. Moreover, the country is characterized by high levels of populist communication, polarization, and low levels of trust in the news media.

193. Levitsky and Ziblatt, 2018.
194. Rid, 2020.
195. Ibid.
196. Humprecht et al., 2020, p. 506.

> Based on the contextual conditions shown by our empirical analysis here, the United States must be considered the most vulnerable country regarding the spread of online disinformation.[197]

While media and technological context has changed, the United States remains its main external threat in the Kremlin's perspective. Not only is the United States the most powerful democratic state, but it is also the leader of global democracy with outsized influence in multinational organizations that keep Russia down.

Combined with the vulnerabilities listed above, then, it is not surprising that the United States has been the biggest and most frequent target of Russian disinformation.[198] Russian disinformation targeting the United States can achieve many objectives simultaneously. A weaker United States means not only a stronger Russia, but also weaker pro-democracy efforts worldwide. Therefore, according to Richey, the sustained global operation beginning in 2013 sought to subvert democracy by:

> (a) dissuading rival political entities, especially the USA and Europe, from challenging Russian kinetic action; (b) generalizing cynicism about domestic and international politics, discrediting the idea of global governance based on international law and norms, and popularizing Russian policy agendas within international populations; (c) legitimating artificially constructed "facts on the ground"; (d) causing dissension within and among states allied against a given Russian action.[199]

This background highlights the importance of the United States' will and capability to mitigate the Kremlin operation's effects. The Putin regime cannot compete in an open, rules-based order, it cannot defeat the United States' capability directly, and so it chooses subversion. The biggest target of a global antidemocratic subversion was to attack the

197. Ibid.
198. Martin et al., 2020.
199. Richey, 2018, p. 109.

United States' will, degrading it over time through disinformation.[200]

The resources and effort Russia has committed to undermining American self-government demonstrates the value they assign to the objective. Through exacerbating conflict and division in the United States, it targets will to undermine capability. This reinforces my framework's logic; capability and will are both important variables that determine states' policy responses, but of the two, will is more important. It is will that that organizes a response to the threat from disinformation. Russian disinformation attacks against the United States shows that the Kremlin shares this assessment; the next section will detail some specific recent attacks that have targeted the United States' will.

Russian Disinformation in the United States

Capabilities and Targets

To understand the United States' response to Russian disinformation, it is first important to understand the Kremlin's attacks. Understanding Russian capabilities and target audiences is important for developing a United States Government response.

As mentioned previously, before invading Ukraine in 2014, Russia committed significant resources planning then conducting a global pro-Putin, anti-West campaign. The Internet Research Agency (IRA) was at the heart of the operation,[201] with over 1,000 people and at least a $25 million budget targeting initially Russians and Ukrainians, then Americans ahead of the 2016 election.[202] The Internet Research Agency was not the only Russian effort in this global campaign, however. The United States Director of National

200. Richey, 2018, p. 109.
201. Gregor and Mlejnková, 2021, p. 85. The Internet Research Agency (IRA; Agentstvo internet issledovaniya), known broadly as the Russian troll farm was founded in 2013 and is the most important symbol of Russia's campaign to spread propaganda and disinformation.
202. DiResta et al., 2019, p. 6.

Intelligence described the complexity of the operation, which incorporated "covert intelligence operations such as cyber activity-with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls."[203] The third-party intermediaries include witting and unwitting agents, including Americans.[204]

The Americans enlisted in this operation did so for several reasons. Some, like Larry King and Jesse Ventura[205] got paid to work producing shows for RT. Others held views that aligned with Russian objectives, so were useful in spreading Russian views organically.[206] Still others, like those who support the global white nationalist movement,[207] the Patriot movement,[208] or secessionists in Texas and California[209] provided American audiences that worked both as targets of disinformation and nodes of amplification. The Kremlin used its troll army in conjunction with American voices that knowingly or not helped advance Russian narratives. It further amplified these voices using automated accounts (bots) which mimicked actual human engagement to game

203. Dew, 2019, p. 156.
204. Bodine-Baron et al., 2018, p. 27. Four potential categories of Russian agents includes "witting and unwitting participants who are motivated to spread messages convenient to Russia's goals for their own reasons—including those simply holding views the Russian government seeks to promote—and therefore provide an additional channel to achieve Russian goals, such as creating or expanding divisions in American society."
205. Ibid.
206. Pynnöniemi, 2019, p. 162.
207. Gregor and Mlejnková, 2021, p. 85. "Another important actor in the spread of disinformation and propaganda is the global white nationalist (or far right) movement, with its own media and communication channels…The traditional neoNazi and neo-Fascist Far Right has been using the Internet since the 1990s to spread their traditional conspiracy theories, including their infamous Holocaust denying. The location of many such websites in the United States is typical due to different limits of freedom of speech"
208. Butt and Byman, 2020, p. 140. "Russian media performs an open and leading role, playing up migrant crime in Europe and other white-nationalist hot-button issues. The ubiquitous 24-hour, government-funded news station RT regularly hosts far-right commentators, helping to infiltrate their ideas into the mainstream. These commentators have included Holocaust deniers, members of the United States-based Christian Patriot movement who reject federal authority, American far-right leader Richard Spencer and other voices once confined to the information wilderness."
209. DiResta et al., 2019, p. 9. "The IRA sowed both secessionist and insurrectionist sentiments, attempting to exacerbate discord against the government at federal, state, and local levels. Content focused on secessionist movements including Texas secession (#texit) and California (#calexit). These were compared to #Brexit."

social media algorithms and promote weaponized information.[210] This mix of capabilities resulted in a cacophony on social media, which percolated into traditional media and drove divisive narratives in the United States.[211] The confusion and division was aimed at lowering American will over time.

According to my framework of will and capability, the Russian attacks reveal the effectiveness of coordinated attacks on will. Capabilities available to Russia are different in the United States than the mix available for use in neighboring states like Ukraine or Finland.[212] The effect of the Internet Research Agency's thousands of employees and tens of millions of dollars was to distract, divide, and dismay a state with hundreds of millions of citizens and budgets in the Trillions. Since the United States is so far away from Russia, and because the United States military is more powerful than Russia's, the Kremlin chose asymmetric weapons like disinformation to attack the United States This relatively small organization coming from a relatively weak Russia highlight why the United States did not demonstrate a high will to defend itself; the United States Government failed to coordinate an effective defense against the threat because it did not take the threat seriously enough. Further, the themes that Russia spread with the capabilities show specific ways that the American system is vulnerable to such a leveraged use of information.

---

210. Polyakova and Boyer, p. 4. Key actors in the campaign included overt actors like RT, Sputnik, and Ruptly TV. There are also covert actors such as: Social media trolls, bots, impersonation accounts on Facebook, Twitter, and Instagram, WikiLeaks, and DCLeaks.
211. Benkler et al., 2018.
212. Radin et al., 2020, p. 2. "The threat of Russian subversion to different countries varies based on the intensity of Russia' interests and the resources available to undertake subversion. In western Europe and the United States, Russian subversive tools appear to be limited to information, cyber, and political ones. In neighboring former communist countries, Russia uses a wider range of military and economic tools."

Attacks Since 2013

According to my framework and the tactics of Russian disinformation, Kremlin attacks in the United States have been attacks on American will. Viewed through this perspective, the disparate target audiences and capabilities from the previous section have one thing in common; each is a resource for sowing division, distrust, and discord. Similarly, the employment of those resources, though continuous for nearly a decade has concentrated around themes and events which seem unrelated. Over time, however, the Kremlin pushes the same themes opportunistically adapted to fit changing events.

The Kremlin found opportunities in changes social media created in the media environment. The themes Russia has pushed in recent years are those which filtered up through the survival of the fittest approach of algorithmic natural selection. Because social media outlets prioritized engagement and humans engage most with intensely with outrage, themes of Russian propaganda were outrageous: racism, anti-Semitism, inequality, pedophilia, satanism, guns, and others.[213] Russian propagandists did not take a moral stance on any of these issues, of course, often amplifying both sides of a contentious issue.[214] Division is desired effect. Ultimately, sowing division and distrust is aimed at a purpose of destroying a system that depends on majority rule, norms for protecting minority rights, and trust that improvement is possible through iterative interactions.[215] The divisive themes were particularly salient in attacking American democracy through regular, planned events and taking advantage of targets of

213. Nimmo, et al., 2020.
214. DiResta, et al., 2019.
215. Levitsky and Ziblatt, 2018.

opportunity.

Planned events, specifically elections, provided a target rich environment for Russia to attack American will. As Mason argued, many of the existing divides exacerbated by disinformation prevents our ability to act collectively; within the United States, partisan identity is increasingly central, aligned with race, religion, education, and other cleavages that make it easy stoke discord.[216] Elections are a heightened time in the United States for two reasons: elections are backdrops against which to drive divisive narratives, and elections are opportunities to distort collective decisions in ways that lead to political self-disorganization by choosing officials who work counter to American interests. Elections are the mechanism by which democracies confer power on leaders. Precisely when Americans come together to address issues, one of its major political parties now actively employs domestic disinformation to seize and maintain power.[217] To the degree that Kremlin propaganda fuels this outcome, it is an example of the Russian concept of reflexive control.[218] The Kremlin targeted multiple American elections, then, as a direct attack on degrading Americans' trust in government through election fraud conspiracies and on distorting the expression of that will by promoting extreme positions and candidates.

Other recent attacks have used unplanned events as new opportunities to push old narratives. The massive Black Lives Matter protests and the COVID pandemic,

---

216. Mason, 2018.
217. Benkler, et al., 2018.
218. Pynnöniemi, 2019, p. 159. "The theory of reflexive control, intensively developed by Soviet military and civilian theorists since the early 1960s, explains and provides practical means for achieving the "self-disorganization" of the enemy. According to V. A. Lefebvre, one of the thinkers behind the theory, reflexive control is 'a process by which one enemy transmits the reasons or bases for making decisions to another.'"

specifically, presented major opportunities to inflame tensions within the United States. The Kremlin has for years prioritized cultivating Black American assets and audiences to exacerbate existing racial divisions.[219] Additionally, the COVID pandemic has presented an opportunity for internal division by pushing medical disinformation, conspiracy theories, and racist disinformation that recalls Soviet themes during the 1980s AIDS epidemic.[220]

These attacks have contributed to existing divisions and made things worse by amplifying extremes. By 2021, election related lies and conspiracy theories pushed the threat of political violence, and physical attacks were both planned and executed across the country. For example, according to Kleinfeld, "From death threats against previously anonymous bureaucrats and public-health officials to a plot to kidnap Michigan's governor and the 6 January 2021 attack on the United States Capitol, acts of political violence in the United States have skyrocketed in the last five years."[221] The attacks all have one thing in common; each is rooted in disinformation aimed at subverting American will by undermining democratic institutions. Democracy depends on the legitimacy of popular will as expressed through democratic institutions.

The successful spread of Russian disinformation in the United States conforms with much of my framework for a low will state with high capability. As a larger, distant state

219. DiResta et al., 2019, p. 8. "The most prolific IRA efforts on Facebook and Instagram specifically targeted Black American communities and appear to have been focused on developing Black audiences and recruiting Black Americans as assets."
220. Nimmo, et al., 2020.
221. Kleinfeld, 2021, p. 160. "An unprecedented number of elections administrators received threats in 2020—so much so that a third of poll workers surveyed by the Brennan Center for Justice in April 2021 said that they felt unsafe and 79 percent wanted government-provided security. In July, the Department of Justice set up a special task force specifically to combat threats against election administrators."

to Russia, the United States failed to develop a will to deal with the threat until the corrosive effects became quite serious. The known Russian attacks on the United States before the election included discrediting President Obama, polarizing existing American divisions about the Affordable Care Act and the Dakota Access Pipeline, and spreading false reports of a chemical explosion in Louisiana.[222] While these attacks were monitored and assessed, that was by an administration and government that believed the impacts could be contained without extraordinary effort.

It was the 2016 Presidential election, however, that got the government's attention. Russia's operations increased before the election to divide Democrats, undermine Hillary Clinton, and support Donald Trump.[223] This is not to claim that the Russian attacks are responsible for Trump's victory. As detailed earlier, the point of the disinformation was not to convince Americans that Trump would be a great president, the goal was to sow maximal division. The outcome was not the goal, generating argument and confusion to weaken America was the goal.

Still, Trump's election was an unexpected opportunity for Russian propagandists. The Internet Research Agency continued feeding division and pushed narratives supporting Trump's judicial nominees, discrediting investigations into Russian interference, attacking Trump's Conservative critics, discrediting American actions in Syria, supporting Texas and California secession movements, attacking Democrats, and bolstering the American alt-right movement.[224]

222. Martin et al., 2020.
223. Ibid.
224. Ibid.

This escalation before and surrounding the 2016 election drove a reciprocal escalation in policy responses. It became evident that the policies taken by the United States government before 2016 were leaving the country vulnerable to manipulation that was now serious enough to influence the system at its highest levels. The next section details how American will and capability explain its suboptimal approach and lack of focus dealing with Russian disinformation until the Kremlin operations became unavoidably brazen.

United States' Response

Will and Capability

While the United States had the highest capability in my sample, its rating for will was low. As shown in Table 15, the United States is by far the world's most powerful democratic state and, as already discussed, the biggest target of Russian disinformation operations. To underscore that point, of the thirteen states in my sample only five states were targeted multiple times by publicly identified Russian influence campaigns. The Netherlands, Germany, and Australia were targeted twice, the United Kingdom was targeted three times. The United States, however, has been on the receiving end of fourteen such attacks.[225] The Correlates of War CINC average for the United States from 2013-2016 was greater than the combined total of all other democracies in the sample

225. Martin et al., 2020.

plus Russia. The United States also topped the Belfer Center's ratings for information control and norms components of their cyberpower rankings.

The United States is targeted so often because it is rife with sharp internal divisions and because undermining the United States also undermines the United States-led rules based postwar global order. With regards to trust among its people, the United States Government averaged 35% trust among its population. That scores ninth of thirteen—just less France and just higher Lithuania. The United States is also considered a "flawed democracy" according to the Economist Intelligence Unit's 2020 ratings and has been trending lower in its democracy score in recent years. The United States first scored as a "flawed democracy" only in 2016, degraded slightly in 2020, and the Economist Intelligence Unit expects that issues with the functioning of government combined with

Coorelates of War CINC			NCPI Ranking (Information Control and Norms)			OECD TrUnited Statest		
	Avg. 2013-16	Since 1991	State	Average		State	Average	
United States	0.13204	Q1	United States	1.0	Q1	Netherlands	61.31	Q1
Russia	0.03786	Max .15630	United Kingdom	7.0		Germany	58.83	Max 80.86
Germany	0.01688	Q2 .01998	Russia	7.5		Canada	58.02	
United Kingdom	0.01433		France	10.0	Q2 9.4	Finland	57.01	
France	0.01374		Australia	11.0		Sweden	55.48	Q2 55.73
Italy	0.01150		Sweden	11.0		Russia	51.57	
Canada	0.00861	Median .0104	Canada	12.5		Australia	45.66	
Spain	0.00764	(Q3 .02281)	Netherlands	14.0	Q3 12.8	United Kingdom	40.42	Q3 44.92
Australia	0.00674		Germany	15.5		France	36.22	
Poland	0.00549		Spain	17.5	Q4 16.0	United States	35.09	
Netherlands	0.00398	Q4 .00543	Lithuania	22.5		Lithuania	33.86	Q4 34.52
Sweden	0.00210	min .00039	Italy	24.0		Poland	33.11	Min 14.57
Finland	0.00151					Spain	29.10	
Lithuania	0.00041					Italy	25.19	

Table 13: Will and Capability Ratings for the United States

low trust in institutions will likely continue in coming years the United States' score trending lower.[226]

Many social divisions exist domestically: race, economic inequality, religious,

226. Economist Intelligence Unit, 2020, p. 44.

regional, educational, among others. Beyond those divisions, though, the structure of the United States system further complicates an effective response to disinformation. Because of the separation of powers, no one agency or entity with the government can unilaterally react. The United States' federal bureaucracy is sprawling. There are myriad departments, agencies, offices, and branches with overlapping responsibilities. They are also human endeavors which means leadership and employment involves inconsistent abilities and motivations. In a word, the bureaucracy is complex. Even when government officials have the will, coordinating an effort across the massive United States government is hard.

Will in the United States is also low because of its geography and Cold War history. The United States during the Cold War was certainly a high will leader of a global containment strategy which eventually helped lead to the Soviet Union's collapse. Russia is a large state, but not one that dictates the global equilibrium. While wars still occasionally broke out, the Cold War can be understood as a stable bipolar order underpinned by power in Washington and Moscow.[227] Washington emerged as a lone superpower, Russia became a power much diminished, debatably regional, power compared to the global influence wielded by the Soviet Union.

This drove a different understanding of the American assessment of threat from Russia. In the 1990s and 2000s, the once all-consuming threat from Moscow dropped down the prioritized list of current and likely future threats. Not only was the threat from Russia downgraded, American strategy was to integrate Russia and China into the

227. Waltz, 1979, p. 182.

existing global order. Quickly following the September 11, 2001 terrorist attacks, the United States prioritized Afghanistan, Iraq, and launched a Global War on Terror against the Axis of Evil.[228] Then, shortly before as Russia was ramping up its global operations to undermine democracy around the world, President Obama announced in 2011 a United States strategy to rebalance—pivoting away from Europe and the Middle East to China and the Indo Pacific.[229] At no point following the collapse of the Soviet Union did the United States focus intently enough on Russia to demonstrate high will to combat Russian disinformation.

There were still opportunities between 2011 and the eventual 2016 election attack for the United States to summon more will to combat Russian influence. In a 2012 Presidential debate, Mitt Romney, the Republican nominee argued that Russia remained the United States' "number one geopolitical foe," despite the Cold War's end, a comment for which the Obama campaign mocked him.[230] Had Romney won that election, he certainly would have led a more establishment Republican party and Donald Trump would probably either have run in 2016 as a Democrat or not at all. Had Russia interfered in a way that might have disadvantaged Republicans, he likely would never have objected to publicly disclosing any election attack. Or, had the 2016 election gone as most people expected it would, a Hillary Clinton administration would likely have taken stronger action against Russia coordinated and supported by Presidential power. In either of these counterfactuals, the United States would have acted as a high will high capability state

228. Frum, 2022.
229. Lieberthal, 2011.
230. Friedman, 2012.

more consistently. Existing structural and cultural prohibitions against American domestic government action would have been less of an impediment to taking the threat seriously if actions across domestic sectors were coordinated from the White House instead of the Trump adminstration's haranguing and denial.

The United States National Defense Strategy in 2018 highlighted the challenge of leading competing centers of authority. Combined with the United States cultural and systematic bias against centralized government power, coordination becomes even more difficult compared to the effort Finland must exert to achieve a comprehensive, integrated approach.[231] For example, most capability is within the Department of Defense (DoD), but it is the Department of State (DoS) which is the statutory lead agency.[232] Public Law 115232 tasked the DoS's Global Engagement Center (GEC) to "direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and foreign non-state propaganda and disinformation efforts."[233] And Public Law 116-92 created "created a Principal Information Operations Advisor within DoD to coordinate and deconflict" with the Global Engagement Center.[234]

The most relevant capabilities to challenge disinformation are illegal for domestic use. For example, the National Security Agency and United States Cyber Command have teams which can disrupt, degrade, or block propaganda networks from launching attacks. Reports following the 2020 election showed that Cyber Command disrupted interference

231. Mattis, p. 5. "structural divisions limit our ability to respond to non-military aspects of adversarial competition. No single United States Government department or agency has primacy in the prosecution of irregular conflict or adversarial competition. We cannot assume unified action will occur on its own. We must pursue it deliberately."
232. Theohary, p. 2. "Within the USG, much of the current information operations doctrine and capability resides with the military."
233. Ibid.
234. Ibid.

efforts by Russa, Iran, Cuba, Venezuela, and Hezbollah.[235] But these security agencies are prevented by Constitutional free speech and privacy rights from taking down domestic networks; the agencies are foreign facing.

This is another challenge to an integrated response from the United States Government; although its capabilities are unequaled, it employs them outside of the United States while the threat from Russian disinformation often gets into American discourse through borderless technology. According to a minority staff report of the Senate Foreign Affairs Committee,

> Russian efforts exploited the seams between federal authorities and capabilities, and protections for the states. The United States intelligence apparatus is, by design, foreign facing, with limited domestic cybersecurity authorities except where the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) can work with state and local partners. State election officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor. [236]

Disinformation can exploit social and legal divisions within the United States' democracy to skirt its high capability and erode its low will from within.

Legend:	Low Will	High Capability	Weakened or no state reaction against external threat
Observed			Employment of state capability to use disinformation tactics against domestic audiences
Inconsistent			Democratic backsliding: broken trust, institutions weaken, reduction in domestic freedoms and rights
Not observed			Social division and struggle between domestic sectors, balance of power determines future direction.

Table 14: Overall Findings for the United States

Given the United States' low will and high capability, Table 16 shows my theory

235. Pomerleau, 2021.
236. Russian Active Measures Campaigns and Interference in the 2016 United States Election, Volumes I-V, 2019, p. 5.

predicts the United States Government response will be insufficient to stem the threat of Russian disinformation. The response will be weakened or nonexistent against the external threat. It will involve the employment of state capability to spread disinformation against domestic audiences. The democracy will backslide resulting in broken trust, weakened institutions, and reduced domestic freedoms. And the country will experience increased social division and struggle between polarized domestic actors where shifts in balance of power produce increasingly incoherent national policy over time. The United States mostly conformed to these expectations, but with some significant exceptions. The next section will detail the United States Government's responses.

External Expectations: Weakened Response

My first expectation of a high capability low will state regards its interactions internationally. Because these states lack will to resist, I predict they will turn inward, responding with weak or no action against an external threat. Here, the United States' actions were mixed. The split will within the United States Government meant that some elements took strong actions while others took no action or outright resisted efforts to even acknowledge a threat.

The United States Government has taken several significant actions against Russian disinformation in recent years. For example, in the months after Russia's attack on the 2016 Presidential election, President Obama and Congress created the Department of State's Global Engagement Center in December 2016 to combat Islamic State and

Russian propaganda.[237] The United States' high scores in the Belfer rankings mostly result from operations against Islamic State, so expanding that effort to include a focus on Russia makes sense. And, Admiral Rogers, as Director of the National Security Agency, attributed electoral interference to Russia during the 2017 French Presidential election. The National Security Agency shared this attribution with France, helping France take the proactive steps it did to mitigate the harm.[238] These actions are more aligned with my expectation of a high will state— one willing to defend not only its own democracy but to help protect democratic norms globally.

Further, the government launched multiple investigations into Russian interference including Intelligence Community Assessments, House and Senate committee investigations, and the Special Counsel investigation led by Robert Mueller.[239] The Mueller investigation itself resulted in dozens of indictments both of Americans, Russian organizations, and Russian military officers.[240] And the United States Congress, even while led by Republicans, rallied veto proof majorities to increase funding to the GEC while escalating sanctions on Russian actors in response to Kremlin attacks.[241] These actions were stronger than my framework anticipates for a low will state.

Still, there were United States Government leaders pushing to do even more. The United States' Combatant Commanders around the world took the rare step of publicly

237. Stengel, 2019.
238. Davis, 2018, and Nance and Reiner, 2018.
239. Davis, 2018.
240. Jopling, 2018.
241. Polyakova and Fried, p. 2. "With significant congressional funding of $64.3 million and an additional $138 million requested for 2021, the GEC has provided funding to independent research groups in Europe and elsewhere to carry out counter-disinformation research and develop monitoring tools."

requesting authority to declassify intelligence in time to disrupt[242] Russian disinformation in future crises and United States Cyber Command has taken offensive measures[243] in elections after 2016 to take the Internet Research Agency offline.[244] These steps are consistent with state actions my framework predicts of a state with high will, not low will like I categorized the United States.

Other United States Government actors acted more in accordance with my framework's prediction for a low will state. The strong efforts listed above were for several years carried out despite public efforts by the most powerful actor in the government and efforts by his allies. The United States' response was undermined by President Trump, officials in the Trump administration, its supporters, and even actors who sometimes also worked to counter Russian disinformation.

Trump himself is and was a consistent peddler of disinformation. As a candidate, Donald Trump was undermining democratic allies in ways that echo Russian attacks on democracy rather than demonstrating the will to support democracy abroad. Candidate Trump fed conspiracy theories about Sweden, for example, creating confusion within a steadfast ally and an opportunity that Russian propagandists seized to advance their corrosive narratives.[245] Though Russian disinformation was only one factor among many

242. Woodruff Swan and Bender, 2021. In a joint letter, the Combatant Commanders requested "help to better enable the United States, and by extension its allies and partners, to win without fighting, to fight now in so-called gray zones, and to supply ammunition in the ongoing war of narratives."
243. Polyakova and Fried, p. 2. Cyber Command uses tools to identify and disrupt foreign disinformation operations in efforts it terms "hunt, surveil, expose and disable."
244. Wigell, 2021, p. 61. "For instance, blocking Internet access to the Internet Research Agency (IRA) in Russia served as a useful reminder of United States cyber capacities. This infamous Russian troll factory reportedly sought to repeat its disinformation campaign from the 2016 United States elections by trying to sow discord among American during the 2018 midterms."
245. Bennett and Livingston, 2018, p. 124. "A faked film inspired the president to cite an imaginary crisis, the existence of which was confirmed by a fake expert – and which now inspired another television team to try to create a real crisis using real people (in a neighborhood crawling with both real and fake journalists) to make it all seem true."

that helped Trump win the 2016 election, from a Russian perspective, that attack on democratic politics was the most successful outcome of the Kremlin's global interference operation.[246] Even after winning election, President Trump refused to acknowledge the threat and publicly undercut efforts at addressing it. This prolonged and deepened the United States' inward focus and destabilized relationships with long time democratic allies and NATO as Applebaum wrote:

> The Trump presidency was a four-year display of contempt not just for the American political process, but for America's historic democratic allies, whom he singled out for abuse. The president described the British and German leaders as "losers" and the Canadian prime minister as "dishonest" and "weak," while he cozied up to autocrats."[247]

This reaction more closely corresponds with my framework.

Finally, it was not only President Trump and his administration that worked to undermine United States Government response. When President Obama brought evidence of Russian interference to Congressional leaders, Majority Leader McConnell politicized a decision to make public the information before the 2016 election. This highlights a miscalculation of the threat, indicating lack of will to take it seriously; in the interpretation most charitable to Leader McConnell, he, like most other people, did not believe Donald Trump was going to win the election. As such, he chose against raising awareness of the attack. But the damage was done. The efforts to influence the elections were politicized and added to internal division while the country remained under attack by an emboldened Kremlin looking to exploit its success.[248] Leader McConnell later led

246. Jopling, 2018.
247. Applebaum, "The Bad Guys are Winning," 2021.
248. Martin, Shapiro, and Ilhardt, 2020.

the Senate to pass veto proof and costly sanctions against Russia for the interference.[249] His decision during the election and embodied the reaction of an actor with low will high capability. He had the power to push back against disinformation but chose not to.

While the government did escalate efforts after the 2016 attack to combat Russian disinformation, those efforts were inconsistent, late, and weakened by the leader of the government. I consider this is a mixed result internationally. In some ways the actions reflected expectations of a low will state. In other ways, the United States demonstrated high will to fight back against Russian disinformation. The response domestically more closely corresponded to my predictions for a low will high capability state.

Domestic Expectations: Self-Disinformation, Division, and Backsliding

The domestic responses to Russian disinformation within the United States have more closely conformed to my framework. The second and third expectations of a high capability low will government were evident. State capabilities became nodes of antidemocratic disinformation. President Trump and administration officials used their influence and the influential reach of official White House positions to become the largest node in a network of right-wing disinformation outlets.[250] The President and others used their power to spread lies at an unprecedented rate throughout his campaign, administration, his unsuccessful 2020 bid for reelection, transition to his successor, and continue as of this writing.

His leadership shows the danger of self-disinformation. The National Intelligence

249. Wigell, 2021, p. 61. "For instance, the sanctions against Russia have led to considerable costs for the Russian economy. By depriving Russian state-controlled banks and companies of an important source of long-term financing, credit costs have gone up and investment contracted. According to the International Monetary Fund (IMF), sanctions have reduced Russia's growth rate every year in 2014–18 by 0.2 percent."
250. Benkler, 2018.

Council released an unclassified retroactive report on the 2020 election which highlighted foreign threats to that 2020 election. Despite the United States President's denials and false claims, the report highlights the threat of disinformation and is mostly about Russia.[251] Instead of having a government led by a president defending American interests, the administration was undermining institutions and trust to advance its own narrow interests of power maintenance.

At this point, it is no longer necessary for the Kremlin to develop and seed disinformation in the United States. Rather, some Republican propagandists are doing the hard part for Russia. Trump and a small but influential group of Republicans was even vocally pro-Putin in the lead-up to the 2022 Russian war of aggression in Ukraine.[252] This domestic adoption of pro-Russian tactics further degrades effective governance, lessens trust, and decreases American will. In fact, lying has become so central to the American right-wing, that now the Kremlin just adopts and amplifies disinformation emanating from United States' outlets for use in manipulating Russian domestic audiences.[253]

There has also been ample evidence of the third expectation of a low will high capability state. Disinformation that amplifies and mimics Russian disinformation has resulted in further loss of trust, weakened institutions, and erosion of democratic norms. Former President Trump used disinformation as a technique to build and maintain power then used that power to facilitate a systematic effort erecting barriers to opposition.

---

251. Applebaum, 2021.
252. Thompson, 2022.
253. Ibid.

Within his party he has marginalized anyone perceived as insufficiently loyal. During the election and in the middle of a global pandemic, he worked for months to undermine trust in the United States Post Office and mail-in ballots to raise doubts ahead of the election.[254] This campaign echoed Russian tactics of smearing the legitimacy of elections by appealing not to evidence or logic, but to base emotion.[255]

The months of seeding mail-in fraud disinformation also set the stage for supporters to accept fact-free challenges to the result.[256] President Trump and his team lost dozens of legal challenges, some so frivolous that lawyers bringing the cases have faced professional discipline, financial sanction, and potential disbarment for their efforts.[257] The efforts sowing discord resulted in a violent attack on Congress' certification of Trump's defeat.

The United States' democracy entered this period with significant issues in its democracy, but throughout the period disinformation became central to a Presidential administration and one of two major political parties. By 2020, that democracy continued to decline and the country even began experiencing unprecedented political violence based on lies and threats against even low-level election officials. Nearly 80 percent of normally anonymous elections administrators surveyed in 2021 now wanted security.[258] This shows strains on democracy in multiple ways; threats of violence are likely to

254. Benkler et al., 2020, p. 1.
255. Bjola and Papadakis, 2020, p. 641.
256. Bennett and Livingston 2018, 124. Repetitive lying creates strategic deception through "systematic disruptions of authoritative information flows…that may appear very credible to those consuming them"
257. Molinaro and Moss, 2021.
258. Kleinfeld, 2021, p. 160. "An unprecedented number of elections administrators received threats in 2020—so much so that a third of poll workers surveyed by the Brennan Center for Justice in April 2021 said that they felt unsafe and 79 percent wanted government-provided security."

discourage turnout and it can no longer be said that the United States has an unbroken tradition of peaceful power transitions.

These effects are evidence of democratic backsliding, consistent with expectations for a low will high capability state. The United States' ability to function is being hamstrung by including more and more political actors in seats of power who are outright conspiracy theorists themselves, or who are failing to check the spread of conspiracies and disinformation from their colleagues. If this trend continues, will over time will decrease; a potential future disinformation attack like Trump's big lie has increased chances of success to the degree that supplicants will be in position of authority when it happens again.

The last expectation for low will high capability response is increased social division, struggle between domestic sectors, and that the balance of power determines the state's future direction. This expectation was also evident.

Others stepped in when the administration failed to act. Campaigns, now operating in an environment where disinformation is increasingly utilized by Americans against Americans, hire expensive cyber and information experts to help navigate threats.[259] This raises the cost for participating in politics and increases the threshold that candidates must clear even to compete for office, further undermining democratic participation. Civil society organizations like the Atlantic Council Digital Forensics Lab stepped up to expose and counter disinformation as a means of combatting Russian hybrid attacks against democracy.[260] And other government organizations took actions of their own

259. Davis, 2018.
260. Hanzelka and Pavlikova, 2021.

accord. In September 2017, the Department of Homeland Security informed 21 states that Russia had attempted to access their state voter databases.[261] Officials from the Obama administration and even the early Trump administration including Secretaries of State and Ambassadors to the United Nations noted the uptick in Russian "hybrid warfare" operations around the world.[262] Finally, as already pointed out, a veto proof majority in the then-republican controlled Senate imposed increased sanctions on Russia ahead of the 2018 midterms.[263]

But President Trump was already consolidating power within the Republican Party and anywhere Trump held sway, efforts to punish Russian propagandists were minimized, opposed, and silenced. His power in the party only grew over time and the degree to which he or other similar-minded leaders control levers of power, the United States will be less effective in confronting external disinformation with the considerable capabilities it possesses.

Right up until the 2022 invasion of Ukraine, the former President was still praising Russian President Putin as a genius. And, as the lie outlasts the liar, a small but vocal group of Republican officials and media outlets continue spreading pro-Russian, pro-Putin propaganda. The main adversaries in the fight for United States democracy are now domestic constituencies competing to undermine its democracy using lies and disinformation in patterns easily recognizable in Kremlin operations. American security agencies will keep disrupting Russians externally, but it will need to be non-state actors

261. Davis, 2018.
262. Hall, 2017 and Jopling, 2018.
263. Jopling, 2018.

that address the threat from within as domestic actors have internalized Kremlin tactics. Overall, the trends in United States domestic response to Russian disinformation has been more closely aligned with my framework's expectations.

Lessons Learned

My framework's predictions for the United States Government's response to Russian disinformation since 2013 was mixed. In some ways the response conformed with expectations. For example, Russian tactics employed within the United States have damaged American democracy. Democratic rankings for the United States system have decreased, trust continues to sink, and protections for individual freedoms and rights have been under attack. Also, the last several years have seen multiple cases of disinformation intensifying divisions, fueling threats of violence against election officials, and motivating political violence at the Capitol. These trends are consistent with predictions of a state with great capability, but no will to use those capabilities against Kremlin attacks on democracy.

The other expectations were not as clear. These expectations were: 1) weakened or no state reaction, and 2) employment of state capability to use disinformation against domestic audiences. The state response was indeed weakened during the Trump administration, specifically, since it was led by a Chief Executive who publicly ridiculed elements within the government who were acting against Russia. But those actions went ahead anyway, many times helping allies protect democracy internationally. This expectation is more aligned with what my framework would predict for a high will state. Further, while President Trump and his administration did use their positions and

influence to mobilize their supporters through disinformation, the major capabilities that account for the United States' high Belfer ratings remained legally blocked from operating domestically. The inconsistency in these two expectations show that my framework is incomplete.

Considering the United States as a low will high capability state is too simplistic. There are significant elements within the government, especially those within the relevant parts within Department of State, Department of Defense, the Intelligence Community, and Department of Justice that consistently displayed high will. That will is mostly focused externally. Kremlin tactics at their most effective find authentic domestic voices to spread harmful narratives. To the degree that Pro-Russian, antidemocratic narratives spread from within the United States, this circumvents the best American Government capabilities to respond. And it is also inadequate to consider only State capabilities. Even though the capabilities which exist in the United States are greater than any other state in my sample, there are in the United States many non-state capabilities with expertise in combatting disinformation. Tying my two case studies together, for example, it was an American University to which the high will Finnish Government recently turned for training its officials.

My framework could be improved by accounting for other factors including structural constraints that, by design, make it difficult to achieve unified effort. In the United States system, absence of unified effort is not necessarily evidence of absence of will. Similarly, because state capabilities are foreign facing, my framework would better explain the United States' response if it made a clearer distinction between foreign and domestic

spheres. To do this, my framework would have to expand to include response from non-state actors. Although they do not command resources on a level comparable with the United States Government, Civil Society Organizations (CSO) still have important parts to play. CSOs have been effective in exposing disinformation by attributing attacks, through investigative journalism, and in analyzing publicly available information.

Finally, as in several of the other state responses I evaluated for Chapter 3, the United States' response has a temporal component. Early in the period, the threat was not as apparent as it should have been. The 2016 election, electoral fraud conspiracy theories, and COVID all provided ample opportunities for antidemocratic propaganda. As a result, American democracy declined even to the point of violent insurrection. But the situation will change. The final section outlines what is likely to come next.

Future Challenges

According to my framework and lessons learned researching this case study, several themes emerge which will likely continue in upcoming years.

First, the gap in the United States Government's foreign facing capabilities and domestic limitations is fundamentally rooted in expansive rights for individual citizens. This gap will persist and will bifurcate the United States response moving forward: the government will fight Russian disinformation internationally, CSO will fight it domestically.

The foreign facing security posture of American security agencies is not a historical accident. The country was founded on the idea that government derives power through periodic conferral by the people. Keeping defense and intelligence focused outward is

meant to protect individual rights and freedoms domestically, emphasizing a belief that an open society is ultimately the best long-term security against tyranny. The norm is a significant barrier to achieving anything like unity of action in the United States. Such unity typically only happens after a shocking attack like Pearl Harbor, or 9/11. Disinformation, on the other hand, is designed to prevent unity through plausible deniability and stoking division. So, the future threat of disinformation will not be a shock, rather it will continue as a long-term infection aimed at United States will. Offensive government capabilities will remain focused abroad and, especially when not led by a President who is himself a node of disinformation, will look more like a high will high capability state internationally. Other capabilities will continue to develop domestically to combat disinformation.

Just as Kremlin disinformation aims to eliminate the line between war and peace, it also seeks to blur the line between foreign and domestic. The threat from Kremlin tactics has been internalized and no longer requires the Kremlin to continue having an impact on American democracy. Lies outlive the liar and disinformation in an American context does not require a President Putin or President Trump. Other groups will continue using lies to motivate, organize, and radicalize counterpublics in the United States. These groups include the Patriot Militia movement, white supremacists, Christian nationalists, and other groups who, for other reasons beyond their speech, can bring government capabilities to bear. To the degree these groups do so in furtherance of crimes, especially with international links, the United States Government capabilities can be used to disrupt their efforts. But, more fundamentally, it will not be government capabilities that decide

the effectiveness of American resistance to disinformation. CSO will play an increasing role in understanding, exposing, and discrediting domestic propagandists. The government will focus out, Civil Society will focus in. There will be several upcoming tests for this arrangement in coming years.

Fly has described COVID as a "playground for disinformationists."[264] From the perspective of Kremlin-backed propagandists, that will likely be true for the period beginning shortly before the 2014 invasion of Ukraine and, fittingly, ending shortly after Russia's 2022 escalation Ukraine. The scale and scope of a highly resourced Russian disinformation operation was only matched by the degree to which the United States Government and society were uncoordinated, disinterested, and unprepared for response.

The United States has the capabilities to fight disinformation. Abroad, the United States government is showing leadership in blunting Russian disinformation in Ukraine. The government and America's allies have clearly learned lessons on preempting Russian narratives. The United States Government has looked more high will than low, leading a unified diplomatic campaign with the same allies the Kremlin has targeted for division: NATO and the European Union.

There will also probably be yet unknown crises. Every crisis is an opportunity for adaptation of disinformation exploiting existing divisions, not a new phenomenon every time.[265] If enough domestic leaders continue to employ disinformation domestically,

264. Nordlinger, 2020. "Authoritarian regimes can distract from their own failures… by assigning blame to democracies, chiefly the United States. Russia has also seized the chance to pit allies against one another."
265. Jackson and Lieber, 2021, p. 52. "With disinformation accompanying the crisis, there are two choices: (1) to either view adversary sponsored COVID-19 disinformation and misinformation as a separate information campaign, or (2) to realize that COVID-19 disinformation and misinformation are opportunistic adaptations by adversaries who aim to reinforce existing narratives."

divisive and hyperemotional narratives will continue to stoke unrest. Snyder describes how this turn away from truth is a turn towards American fascism. Specifically, Republican presidential candidates in 2024:

> will presumably have a Plan A, to win and win, and a Plan B, to lose and win. No fraud is necessary; only allegations that there are allegations of fraud. Truth is to be replaced by spectacle, facts by faith. Trump's coup attempt of 2020-21, like other failed coup attempts, is a warning for those who care about the rule of law and a lesson for those who do not. His pre-fascism revealed a possibility for American politics. For a coup to work in 2024, the breakers will require something that Trump never quite had: an angry minority, organized for nationwide violence, ready to add intimidation to an election. Four years of amplifying a big lie just might get them this. To claim that the other side stole an election is to promise to steal one yourself. It is also to claim that the other side deserves to be punished. Informed observers inside and outside government agree that right-wing white supremacism is the greatest terrorist threat to the United States…[when] violence comes, the breakers will have to react. If they embrace it, they become the fascist faction.[266]

If Trump or someone else with low will to combat Russia wins the 2024 election, then it is unclear whether the United States will continue to demonstrate high will internationally. It is also likely that the country will not show much will domestically either; should one of Snyder's so-called breakers succeeds in taking power domestically, that will occur in a bureaucracy that is still dealing with years of neglect and attack from within by Trump appointees.[267] Further, a leading Ohio Senate candidate underscored recently that the attack on the already hobbled bureaucracy should be escalated dramatically:

> 'I think Trump is going to run again in 2024,' he said. 'I think that what Trump should do, if I was giving him one piece of advice: Fire every single midlevel bureaucrat, every civil servant in the administrative state, replace them with our people.'

266. Snyder, 2021.
267. Lewis, 2018.

> ‘And when the courts stop you,’ he went on, ‘stand before the country, and say—' he quoted Andrew Jackson, giving a challenge to the entire constitutional order—'the chief justice has made his ruling. Now let him enforce it.’[268]

This would continue the assault on American democracy so far highlighted by the January 6 attack on the Capitol. If that assault succeeds it would be another major weakening of American institutions, further degrading the bureaucracy’s will to address external threats.

The threat previously posed by Kremlin disinformation tactics is now even more dangerous, having been adopted by American actors for partisan gain. Whether power resides in coming years with domestic organizations have sufficient capability and will to bear costs fighting disinformation or those actors who calculate that the benefits of using disinformation domestically outweigh its costs, will determine whether the United States has a chance to bounce back as a leading democracy or a further move towards authoritarian rule.

268. Pogue, 2022, Quoting Trump-endorsed candidate for Senate in Ohio, J.D. Vance.

CHAPTER 6
CONCLUSION

Summary of Findings

Russian disinformation continues to threaten democracy globally. A massive escalation in 2013 was a logical exploitation of success the Kremlin found after roughly a decade of the Putin regime's experiments controlling the Russian domestic information environment, subverting its neighbors, and adapting tactics to advances in media environments. Different democratic states responded to the Kremlin's global operation with varied combinations of will and capability.

My framework predicted responses based on grouping states according to their will and capability endowments. The framework was generally a good predictor of responses for a varied group of states that Russia attacked from 2013-2020. By studying the thirteen different states, some patterns emerged. I learned that of the two endowments, will was the more important variable. All states in the sample suffered democratic backsliding whether they had high or low capability. Although some states with high will also suffered setbacks during the Kremlin operation, it was the high will states that innovated new approaches to pushing back on Russian disinformation which appear to be paying off in Ukraine in 2022; more on that later.

Though the framework was generally a good tool for predicting the kinds of responses each kind of state would choose, the case studies provided much greater context on will as a mechanism—why will is so high in Finland, why the United States

will was so bifurcated, and why one of the smallest states in the sample succeeded in resisting when the largest struggled.

In Finland, for example, the country's high will long predates the latest Russian influence operations. Finnish history is one long story of living in the threatening shadow of its much more powerful neighbor. Finland has had to fight costly wars to maintain its independence. It spent the decades of the Cold War fending off intensive influence operations from Moscow and even after the collapse of the Soviet Union, never let its guard down. Finland understands the threat posed by Russia and prepared a resilient society long before the Kremlin adopted its tactics to a changed context. In many ways, Finland responded well because it has cultivated a unified and flexible population with a clear understanding of Russian aggression. That shows in Finland's high Organization for Economic Cooperation and Development Trust rating and explains how one of the lowest capability states in the cross-national survey is also one of the few success stories resisting the Russian disinformation onslaught.

The United States case study generated different takeaways for the framework. In contrast to Finland, the United States has consistently downplayed the threat from post-Cold War Russia. Though Russia is not a peer competitor with the United States like the Soviet Union used to be, Russia has adapted to the changed power dynamic by adopting asymmetric capabilities like disinformation to close the growing divide. Foreign facing elements of the United States Government have the demonstrated ability to disrupt propaganda networks, but the attacks in Russia's post-2013 operation moved into the American domestic sphere and exploited gaps and seams in the United States' system.

The best government capabilities could not operate against domestic networks because of Constitutional restrictions. This means that the United States has high will, but in some ways looks low will by not acting stronger in a domestic context.

Why This Matters

As Polyakova and Fried point out, democracies have learned through a decade of attack:

> Unevenly, but steadily, a structure for democratic defense against disinformation is emerging, consistent with the principles of transparency, accountability, and respect for freedom of expression. It includes: a growing network of disinformation detectors (led by civil society sometimes informed by government agencies); social media companies (responsive to public and legislative pressure) that constrict disinformation on their platforms; an informed media that exposes disinformation; and, potentially at a next stage, a regulatory framework that seeks to filter out inauthentic and deceptive behavior.[269]

Many of the democracies in the cross-national survey, even the low will states, over several years came to recognize the threat posed by a flood of disinformation. It will take time to adapt to the problem. And while democracies adapt, so will propagandists. Researching this dissertation, several lessons became clear that indicate the need for democracies to prioritize improving will and building capabilities resisting disinformation.

First, whether governments under attack from Kremlin disinformation acknowledge it or not, Russia uses information as a weapon targeting will. Lucas et al., for example, describe this as

> perhaps the single most important aspect of information operations: they should not be seen in isolation, but as part of wider influence operations that use political, economic, legal, and other tools to exacerbate ethnic, cultural,

269. Polyakova and Fried, 2020, p. 2.

demographic, diplomatic, linguistic, regional, and other divisions.[270]

States invest in defending their populations against any number of threats, disinformation should be among them. And disinformation attacks serve multiple roles for the attacker. It is a weapon for organizing subversion, a tool for making democracies act counter to their self-interests, or can be active measures aimed to achieve an inherent political effect.[271] Recognizing the threat is obvious now— both after the sustained Russian campaign against the West since 2013 and particularly after the shock of the Kremlin's 2022 escalation in Ukraine.

Second, there is a temporal mismatch between attackers and defenders. Disinformation attacks have not been constant, the tactics have adapted over decades with changes in technology. Each time a new medium emerges, some actor or actors, such as the Kremlin, adapts to changes to weaponize lies for the purpose of organizing extremists, dividing opponents, and conducting political attacks. The techniques never go away, but their use ebbs and flows while society sorts through transformational changes in the information environment. The shock of recent operation spurred governments to action. By the 2020 election, the United States, for example, had effectively taken the Internet Research Agency offline. After the shocks of the 2010s attacks and Russia's aggression in Ukraine, the threat will continue because the goal of subverting the West will not disappear.

Third, understanding how to maintain will and capability to resist Russian

270. Lucas et al., 2021.
271. See Pynnöniemi, 2019, p. 156 for discussion of information as an organizational weapon, achieving reflexive control, and conducting Active Measures.

disinformation matters because other actors have studied Russian actions and seek to mimic its malign influence. These actors include the Chinese Communist Party, which since 2017 has shifted away from an information operations charm offensive toward a more Kremlin-like aggressive use of disinformation to subvert the West.[272]

Although Russian cultural expertise gives it advantages identifying and exploiting social divisions in multiple states, the tactics could still be useful to the different strengths of the Chinese Communist Party. If Chinese propagandists committed to a global operation like Russia's, the effect could be even more pronounced because China would do so with significantly greater capabilities. Its more systematic, far-reaching, and tightly controlled set of tools could seed messages with even greater resourcing than Russian intelligence arms and organizations, while at the same time allowing for a more robust defense against Western countermeasures.[273] Globally, a Chinese operation might be even more of an issue for democracy than Russia's 2013 operation.

Further, the actors pursuing disinformation as a strategy for subversion are not limited to foreign actors. Modern communications technology blurs the line between domestic and some domestic actors see it in their advantage to undermine democratic governance.[275] Bola and Papadakis summarize the internalization of Kremlin tactics:

> The formation of 'unruly' counterpublics, some of them with a clear antidemocratic profile, is a tangible result of disinformation… Counterpublics are not only about subordinated social groups seeking to call attention to progressive issues in an effort to expand the agenda of the public sphere. As our study shows, counterpublics are also about groups constituted online and empowered by digital platforms, seeking to use themes and topics, often in

272. Charon and Jeangene-Vilmer, 2021.
273. Ibid.
275. Polyakova and Fried, 2020, p. 2. "Purveyors of disinformation have grown more sophisticated and their tactics continue to advance. The line between domestic and foreign disinformation has blurred, with Russian agents using local actors as proxies to carry out disinformation operations."

> alignment with the digital propaganda of a foreign government, to undermine or even block the functioning of the public sphere.[276]

Understanding how disinformation works and how to respond matters because the universe of attackers is growing, not shrinking. Two events largely outside the main scope of this project highlight how future events will impact democratic will and capability: the COVID-19 and the 2022 Russian war in Ukraine.

Shocks: COVID and Ukraine

For developing a workable scope for this dissertation, I chose to focus mainly on 2013-2020. The period is important to studying Russian disinformation because it covered a period of Russia's significant escalation attacking the West with weaponized information exploiting conflicts within and between democracies.[277] The escalation coincided with Russian invasion of Ukraine to cease that state's momentum favoring greater integration with Europe and disfavoring its ties with Russia. Disinformation was part of achieving strategic surprise enabling the annexation of Crimea.

The Russian operations of the period had some very significant effects. Not only the twin democratic disasters of Brexit and President Trump, but also large and small impacts felt by every state in my cross-national sample. The effects, relatively cheaply achieved, were sure to spread. The period closes with the beginning of 2020, as COVID exploded into a pandemic. By then, Russian tactics had proven themselves as effective means to the ends of disrupting democracy. Other state actors like China, Iran, Venezuela, and

276. Bjola and Papadakis, 2020, p. 657.
277. Haynes and Scott, 2021. Quoted Thomas Rid, What Russians mean "by unresolved contradictions is frictions, for example nascent antisemitism in Germany in the 1960s or unresolved racial tensions in the United States also in the 1960s or even today, and then designing and driving a wedge into those cracks in order to pry them open— for example to drive a wedge between West Germany and the United States or between NATO allies."

Hezbollah in Lebanon adapted Russian techniques and antidemocratic segments within democratic societies did too.[278]

The isolation, confusion, uncertainty, inequality, and fear accompanying the pandemic made COVID a "playground for disinformationists."[279] The COVID pandemic shows that while events change, disinformation themes repeat. According to a British expert on Soviet strategy, the Russian Government is using the pandemic and medical disinformation to continue driving wedges into many of the democracies in my sample:

> There's a reason why countries with with Russia has an argument find themselves facing public health crises because of well funded and well organized anti-vaccine campaigns. It is all just a measure to destabilize and erode and subvert adversary societies and not necessarily for any particular political outcomes.[280]

Russia has sown disinformation (incorrect and with intent to harm) and amplified misinformation (incorrect but not meant to harm) to create confusion and conflict around during the pandemic. Public health measures, which adapted as officials worked to understand data during a rapidly changing pandemic, and vaccines, which are an existing controversy for an already unruly minority of Americans, created a great opportunity for malign influence. Approximately one million Americans have died from COVID at the time of this writing. Future studies could attempt to define the number of those deaths attributable to disinformation and misinformation, but the number is not zero.

Also, supporting my conceptualization highlighting trust in government as an important variable for predicting state responses to disinformation, a 2022 article in The

278. Pomerleau, 2021. And Wigell, 2021, p. 49. "disinformation campaigns have become increasingly evident since the 2016 United States elections and have stepped up in the midst of the COVID19 crisis. Russia, and increasingly China, are deploying disinformation to aggravate the public health crisis in Western countries."
279. Nordlinger, 2020. Quoting Jamie Fly.
280. Haynes and Scott, 2021. Quoted Keir Giles.

Lancet attributed lack of trust in government as a major contributor to excess death through low vaccination rates and preventable death.[281] The pandemic, then, just became a more immediately lethal vector for disinformation. The attack here is an active measure; information used as a direct attack.

The pandemic has also been an opportunity to use disinformation as an organizational weapon. Medical disinformation has been twisted into well-funded anti-vaccination campaigns and anti-government trucker rallies in Canada and the United States. The rallies have caused economic disruption and increased dissatisfaction, but also have been an effective rally point for disgruntled segments of society to meet, raise money, and plan future actions. In the name of repealing mask mandates, many of which have already been lifted, these rallies are an example of disinformation creating division within society setting the conditions for further deterioration of democratic will in the long term.

Finally, other antidemocratic actors, having seen the impact of Russia's 2013 campaign, began adopting similar techniques. China, for example, has changed its operations to become more like Russia. Since 2017 the Chinese Communist Party has been less focused on maintaining a positive image around the world and has instead been more oriented on aggression and coercion[282]. The disinformation surrounding the

281. "Pandemic-preparedness indices, which aim to measure health security capacity, were not meaningfully associated with standardised infection rates or IFRs. Measures of trust in the government and interpersonal trust, as well as less government corruption, had larger, statistically significant associations with lower standardised infection rates. High levels of government and interpersonal trust, as well as less government corruption, were also associated with higher COVID-19 vaccine coverage among middle-income and high-income countries where vaccine availability was more widespread…"

282. Charon and Jeangene- Vilmer, 2021. "For a long time, it could be said that China, unlike Russia, sought to be loved rather than to be feared; that it wanted to seduce, project a positive image of itself in the world, and arouse admiration. Today, Beijing has not given up on seduction, on its attractiveness, and on its ambition to shape international norms. Not "losing face" remains very important for the CCP. And yet, Beijing is also increasingly comfortable with infiltration and coercion: its influence operations have been considerably hardened in recent years and its methods increasingly resemble Moscow's."

pandemic has had advantages spreading far and wide like the virus; the world moved more online than before, people suffered and were afraid, and many people were angry about disruptive public health actions taken to prevent needless death. The environment was permissive for propagandists to target dissatisfied groups and to drive wedges within and between democracies.

While the pandemic has been a pessimistic episode since Russia's 2013 operation that shows disinformation works even with a high death toll, another recent event offers reasons for optimism. In 2022, the Kremlin attacked Ukraine again and the response from Western democracies has so far shown that the United States, the European Union, and NATO have adapted since 2013-2014 annexation of Crimea, rallying the will to put Russia on the defensive competing in the Western information environment.

The lead up to Russia's attack on Ukraine has demonstrated that indeed many Western governments have applied lessons on combatting the Kremlin's disinformation. In 2021 and 2022, the Kremlin again escalated having already invaded in 2014. The Russian Army mobilized large escalation included a large information component. So did 2013. But this time, Western democracies were alert to the threat.

The difference between the operations is stark. Even before more troops invaded, the Kremlin employed cyber-attacks and disinformation targeting the Ukrainian resistance. The United States, NATO, and the European Union have been more unified in response to this aggression than perhaps the Kremlin assumed would be true. The United States, particularly, is now able to contribute much more like a high will and high capability state. Because the attack is not happening within the United States and because the

President is not a major node of right-wing propaganda, the United States is able to commit its world class capabilities to the effort.

Russian disinformation has been called out before Russia has been able to deploy it. Multiple intelligence agencies especially in the United States and the United Kingdom have preemptively called out multiple potential Russian disinformation operations before they have even been launched, depriving Russia of the strategic surprise that it enjoyed in 2013. This seems to indicate that states in my sample are displaying a new seriousness to combat the threat.

On the other hand, influential right-wing propagandists like Tucker Carlson in the United States have continued pushing pro-Putin disinformation. The Republican party elite has mostly rallied to support Ukraine, but there remains a vocal minority including several Congressional Representatives and a former President that shows antidemocratic voices still hold sway in the party.

This is the dynamic which will most likely be the clearest evidence whether the United States has hit an inflection point in democratic decline or if it will yet decay further. So, the information space remains contested. The Biden administration has been aggressive in calling out Russian disinformation at several points during troop buildup around Ukraine and throughout diplomatic efforts in 2022. This is a deployment of United States capability to bolster international democratic will to fight a war built on disinformation.

The current crisis in Ukraine did not start in February 2022, but it escalated President Putin's 2014 invasion. Invading Crimea in 2014 was a serious escalation, not only for its

immediate violence against Ukrainians, but also for long-term corrosive information attacks against the West. Of note, Ukraine did not appear in my cross-national survey. Ukraine's system according to the Economist Intelligence Unit's measures only narrowly missed earning the same "flawed democracy" classification applied to the United States.[283]

But Ukraine is a NATO Extended Opportunity Partner state, and it has certainly been attacked by Russian disinformation since 2013. In fact, Russian intelligence agencies and the Internet Research Agency have conducted relentless digital operations against Ukraine as part of its global attack on democracy. The operation began as cover for invading Ukraine and, as Nimmo et al noted, since 2014, the most repeated Kremlin theme by a wide margin labeled Ukraine as a failed state. The other two favored themes were that NATO and the West were the true aggressors, and that Europe is weak and divided.[284]

Additionally, the Belfer Center's rankings for Ukraine place it only slightly ahead of Lithuania which ranks lowest in the sample by capability.[285] The shock of 2022 has, in the short term, elevated and unified the West's will to resist Russia. Ukraine, a very low capability hybrid regime moving in the direction of joining the West as a new democracy, is showing a case of extreme will and finding success dominating a narrative battle globally outside of a handful of pro-Russian states.

Western democracies have made strides to defend against Russian influence.

283. Economist Intelligence Unit Democracy Index, 2020.
284. Nimmo et al., 2020.
285. Voo et al., page 12.

President Putin's flood of lies targeted democratic will. That was having an impact. In recent years, the prevailing narrative was one which supported Russian narratives that the West was in decline, that democracy is weak, and that continued rise of authoritarian regimes' power would not be resisted.[286] But again, the aim of Kremlin disinformation is the long-term subversion of global democracy; the logic of my project suggests this will remain true after the short term implications of COVID disinformation or the likely loss of Russian power after so badly misjudging Western resolve over attacking Ukraine.

Moving Forward

Applying my framework to anticipate future trends in disinformation, I believe the logic of my argument indicates multiple likely trends: Russia is likely to double down on its disinformation capabilities, and disaffected domestic populations will continue engaging with Kremlin propaganda as part of a feedback loop which will continue attacking democratic will.

First, whatever the outcome in Ukraine, Russia is likely to continue emphasizing disinformation. The Kremlin's 2022 attack into Ukraine has been a major shock to the world. Western democracies have rapidly come together to punish Russia for its aggression and to deny a disinformation screen for the military campaign. The will shown, both by Ukrainians and Western governments, has been a surprise. Facts on the ground have made Russian lies look ridiculous and Western audiences, confronted with the reality of military assault on civilian targets, are by wide margins rejecting Russian

286. "Fog of falsehood: Russian strategy of deception and the conflict in Ukraine", 2016, p. 42: "deception, both concealment and misrepresentation, aims at intellectual domination – at putting the West in a state of ignorance about Soviet activities and intentions that is linked to a sense of looming power. The desired psychological outcome is to displace faith in self-defence with faith in appeasement"

narratives.

Differently than 2014, Ukraine, with support of the United States and European allies in exposing Russian pretexts early on, has definitively attributed this war to Putin. In 2014, Russia created disunity in NATO and the European Union by throwing up a cloud of confusion. In 2022, Russian troop movements and disinformation tactics were called out repeatedly and beforehand, prebutting Russia's planned pretexts.[287] This clear attribution has provided clear evidence that Russia is a threat and increases states' will to combat Russian disinformation more widely.

The threat has facilitated the very unity within and between democracies that the Kremlin has long targeted for subversion through disinformation. By moving beyond information attack and into physical war, however, he is bringing the West together. States like Finland and Sweden have already signaled increasing desire to join NATO,[288] for instance. The shock from this latest Russian aggression creates a security dilemma for its neighbors.[289] And it has driven a reversal even in Germany's long post-war aversion to militarizing its foreign policy. Now, not only has Germany ended Nordstream 2, it has also announced significant expansion in its defense spending.[290] Russia feels threatened by democracy, so attacks to create a buffer. That has created a moment where not only

287. Lomas, 2022.
288. Milne, 2022. "Russia's sabre-rattling in Ukraine has reignited a debate in Finland about whether the Nordic country should join Nato, defying Moscow's demands that the military alliance limit its expansion in Europe."
289. Haynes, 2017. "Since the end of World War II, Finland has remained relatively neutral when it comes to military and political relations with Russia and the West. While Finland occasionally works with NATO and cooperates with Russia on trade agreements, it almost never fully commits to aligning with either side.[i] This disposition is out of concern that Russia could retaliate if provoked, particularly since the annexation of Crimea in March 2014. Finland's resulting balance between NATO and Russia has created an arena for both NATO and Russia to continue fighting for influence inside the country." And Szymański, 2018, p. 6, "the increasing potential of the Russian armed forces and the military interventions in Georgia and Ukraine have made Finland decide to intensify its defence co-operation with NATO and the USA."
290. Howard, 2022.

are Russian narratives roundly rejected, but where will is sufficiently high to defend against Russia that decades of forced neutrality may no longer be sustainable.

With will so high across the West, it can even seem like Russian disinformation has lost its impact. The lies have become simply too detached from reality for anyone to believe. But this dissertation shows that it will adapt. Russian capabilities still exist, but are themselves disorganized, tied up in short term internal chaos created by their president's newest war and by incoming attacks by actors of a united West. The Ukrainian President and millions of his people are having success advancing their own narratives even reaching into Russian society. Anonymous targeted the Russian government, global media coverage surged to provide rigorous nonstop coverage, and people around the world got engaged. This level of unified effort has overwhelmed Russia's usual success spreading untruth. Unfortunately, maintaining that will is likely to become increasingly difficult. The world's attention will eventually move on, especially once the intensity of the physical attacks decreases. At that point, if President Putin holds on to power, he will in the coming decade, be more incentivized than ever to reach again for weaponized information.

The biggest threat from another such attack would still be disrupting America's democracy and it will reveal whether domestic actors have learned how to combat disinformation in its own democracy. Regular events including the 2022 midterm and 2024 Presidential elections are predictable targets for interference. Following the 2016 election attack, major social media companies like Facebook and Twitter acted independently to curtail the spread of false information. By 2018, the reduction on the

platforms was significant.[291] By 2021, President Trump was banned from Twitter for violating terms of service by encouraging insurrection. By 2024, he is likely to be a candidate, or President-elect, again. This will raise questions about how he should be able to engage with social media platforms.

Although social media companies have recognized the problems posed by disinformation, they continue to resist oversight and any external checks on their outsized power. According to whistleblowers, internal debate at Facebook after the 2020 election and surrounding the January 6 insurrection prove that the companies, at least Facebook, know ways to limit the worst effects of disinformation; Facebook implemented their "break glass" set of rules around the election, tapered the restrictions after the election, then, witnessing the violence being coordinated on its platform reinstated all the protective measures on the day of the insurrection.[292] Former President Obama noted that these companies try to have it both ways: denying to regulators the companies' ability to influence individual users behavior while basing their business models on opposite claims made to advertisers.[293]

Because these companies are so central to the way Americans create and consume information, they should be subject to oversight. Constitutional protections, especially the first amendment, must remain sacrosanct but there are plenty of ways that social media companies can continue running their businesses without threatening democracy. President Obama argued that debate around Section 230 is not likely going to have the

291. Allcott, et al., 2019.
292. Bond and Allyn, 2021.
293. Dwoskin and Scott, 2022.

best effect, but that laws can be designed to increase transparency regarding algorithmic promotion and amplification while encouraging innovation and balancing the companies' needs to protect intellectual property.[294]

And besides social media, other media organizations and civil society actors will need to engage domestically. Traditional media outlets helped allow disinformation to thrive in 2016 by following longstanding norms of professional journalism including elite bias (if the President says it, it is news) and neutral objectivity (both sides deserve equal space to talk).[295] In 2016, Candidate Trump was famously given ample free airtime on television channels, which aired his comments unfiltered and live. Because he established such a pattern of lying throughout his presidency, this dynamic changed and so did his coverage leading up to the 2020 election. Journalists and editors will be tested again in 2022 by a spate of candidates running for all levels of office committed to election lies propagated by the former president. And if he runs again in 2024, the coverage will again be more intense than in 2016, or, now having inspired an insurrection, than it was even in 2020. Filtering, real-time fact checking, labeling, and contextualizing will all challenge media coverage of those committed to disinformation as a tactic to gain and maintain power.

As for Russia, as outlined in Chapter 2, it is the power asymmetry with the West which led the Kremlin to invest in a global disinformation operation in the first place. Even before the 2022 war in Ukraine, Russia assessed it could not win a shooting war with NATO, instead emphasizing investment in weapons to level the playing field. Competing with bigger, richer adversaries made several options attractive. Russia

294. Ibid
295. Benkler et al., 2018.

complemented its already large conventional military capability with advances in asymmetric capabilities: nuclear, cyber, and disinformation. Now that the conventional Russian military appears much weaker than most analysts predicted, Russia will either be forced to accept defeat and diminished power, or it will need to rely even more on its asymmetric capabilities.

Further, increased sanctions and technological advances will make disinformation even more attractive to Russia. Today's version of the Russian military is the result of reforms pursued after its 2008 invasion of Georgia. Reforming the military takes is expensive. It takes money and it takes time. Russia is likely to emerge from the Ukraine war with neither; economic sanctions will degrade the Russian Government's ability to replace, fix, or upgrade its armed forces after taking unexpectedly high damage during the war. And Russia's petro-state economy was already growing slower than its adversaries' economies. By contrast, spreading disinformation is cheap and fast. President Putin will return to use of inexpensive effective efforts like sowing disinformation in democracies. In fact, reports are already emerging of efforts to reconstitute the Internet Research Agency's influence outside Russia by spreading disinformation about the war.[296] The West must maintain sufficient will, especially when the obvious threat of Russian military aggression fades from the news. Disinformation will continue and so must efforts to resist it.

Several recommendations would help maintain the right balance of capabilities supported by sufficient democratic will to resist:

296. Silverman and Kao, 2022.

1. Do not overestimate or underestimate threat from Russia. In the peak years of the Kremlin's global operation, part of its mission was to make Russia and especially President Putin seem more powerful than they were. This drove a form of psychological control that Vindman describes as self-deterrence: unilaterally deciding not to take some actions against Russia for unjustified assessments of Russian responses.[297] After Ukraine, there may be tendency to underestimate Russian capability. This is also problematic. Overestimation and underestimation both distort democratic decision-making and are forms of reflexive control. Instead, Western democracies must move ahead advancing their own dispositive narrative, backed by other elements of state and multinational power, to secure democratic institutions from corrosive information attacks. Threats from Russia should not prevent Finland or Sweden from joining NATO, rather the alliance should speed their membership with all possible haste to limit the time available for Russia to interfere.

2. Avoid responding piecemeal.[298] Many of the Russian attacks repeated over time or from country to country. Attacks are also integrated with physical events, so the response to disinformation should also be integrated with physical means. For example, since 2013 Russia fomented border crises at varying times in at least Norway, Finland, Poland, and Belarus. Each crisis is its own immediate problem, but to highlight repeated attacks robs Russian narratives of power to penetrate Western information filters. Adding context by calling out Russian tactics makes disinformation less likely to spread. Resourcing

297. Vindman, 2021.
298. Richey, 2018, p. 112. "Indeed, a reactive strategy is what the Kremlin desires. Instead, policy-makers—e.g., in the EU—must anticipate Russian information warfare lines of-attack and construct proactive messaging that immediately accompanies any European action."

organizations like NATO's Hybrid Warfare Center of Excellence and Strategic Communications Task Force[299] can help since their mission is to monitor Russian subversion efforts and to advance Western influence through narratives aligned with democratic values. These efforts need to be bolstered by security forces prepared for agitators seeking escalation and incitement. This can help focus Western resolve positively in the face of future efforts to distract and divide.

3. Fight corruption.[300] Fighting corruption impacts Russian disinformation from both ends of an information attack: the sender and the receiver. The Kremlin uses corruption as a message and a means. It is a message in narratives that highlight Western hypocrisy to distract from Russian corruption. It is a means to undermining democracy since the Kremlin courts corrupt Western officials, especially in right-wing parties, to weaken democracies from within.[301] Steps taken to increase transparency and government accountability are win-win to combat disinformation: decrease Russian capability while increasing democratic will.

Second, the will and capability framework suggest that long-term democratic will is going to remain under threat from Kremlin tactics and techniques, even when attacks do not originate from within Russia. The 2013 operation succeeded in laying a blueprint for subversion. The methods will be taken up by foreign adversaries and disgruntled

299. Ibid. "the EU's Eastern StratCom Task Force should be dramatically upresourced and scaled-up so that it can effectively persuade susceptible populations in the Baltic states and Eastern Partnership countries that a better future lies with Brussels rather than Moscow."
300. Standish, 2017, p. 6. "In Ukraine and Georgia, Russian propaganda often amplifies and distorts the very real problem of state corruption, seeking to destroy confidence in pro-Western political parties."
301. Pomerantsev and Weiss, 2014, p. 20. "Putin's Russia cooperates with European far-right parties partly because the latter help Russian political and business elites worm into the West economically, politically, and socially… the far-right's racism and ultra-conservatism are less important than the far-right's corruptibility."

domestic actors in democracies, especially in the United States. The United States foreign facing government capabilities will continue to create domestic gaps within the most powerful democracy.

Corrupt actors are likely to find Russian support. This support can take several forms ranging from retweets and message amplification to financial and operational support of subversive active measures. Right wing extremists are likely to continue using disinformation to organize online, coordinate internationally, and advance anti-democratic efforts. In the last few election cycles, for example, violent threats against election officials, school boards, and Congress have been rooted in disinformation about COVID and election fraud.

Issues will change moving forward, but the tactics will be the same disinformation will be used as: organizational weapon, reflexive control, and active measures. Returning to trucker rallies show how these tactics play out in a non-Russian context. The rallies are organized around a lie. It does not matter what the lie is; rally planning predated COVID, for example, but came to be organized around mask and vaccine mandates. Eventually they have become a venue for a mix of right-wing grievances.[302] The rallies are now physical events that inspire and radicalize attendees while building networks for future action: this is an organizational weapon. The rallies are aimed at stressing local officials and police, ideally creating a heavy-handed response or incident that can be characterized as government overreach: this is reflexive control. And the rallies are physical disruptions of the communities where they are allowed to occupy: this is employing active measures.

302. Homans, 2022.

The same principles apply to the January 6th, 2021 insurrection: the rally was an organizational weapon, sought reflexive control by precipitating armed conflict with armed security forces, and actively prevented the United States Congress from its work certifying President Trump's loss. Events like the trucker rallies and Trump rallies will continue weaponizing lies using Russian tactics and no longer require Russian involvement. The biggest challenge to democracy is now a challenge from within the United States. Within the American context, my framework shows that the will and capability exist to confront this challenge, but most of the effort will have to come from civil society.[303] The following are a list of ideas and recommendations for likely responses from both government and civil society organizations in coming years:

1. Support free media with transparency and competition. As Polyakova and Fried argue that "journalists, activists, and independent investigators can be the most effective tool of counter-disinformation. It is asymmetric — it does not directly counter disinformation — but plays to the greatest strengths of free societies dealing with authoritarian adversaries: the inherent attraction, over the long run, of truth."[304] Since the United States Government capabilities are limited domestically, the country should put its resources to promoting its most effective capabilities, which has would have the added benefit of improving democratic norms.

Regarding social media, changes to the law should not be limited or even focused on section 230. Social media has been more responsive to disinformation attacks since their

303. Sheives, 2022. "we have been looking for the solution in the wrong place. Civil society, not governments or social media companies, can best diminish disinformation. But these civil society organizations need equipping, and their tools need sharpening."
304. Polyakova and Fried, p. 2

poor showing in 2016, but we should not trust our democracy to a small handful of firms whose underlying motivation is profit. The United States' first amendment protections prevent its legislating content moderation in any meaningful way. But, there is room for better regulation requiring transparency and competition in social media. As DiResta has said, "free speech is not the same as free reach."[305] Anti-trust laws and disclosure requirements regarding algorithmic promotion should be part of a strategy moving forward.

2. Support activities and organizations that foster crosscutting identities.[306] When Americans start seeing other Americans not as existential threats, but as people who must figure out how to live in the same country, compromise becomes necessary. Division can easily be demagogued by appeals to populist nationalism, so bringing Americans together should not be by distorting foreign threats, say from China, for example. Rather, creating and supporting community service organizations that work to bridge political, economic, and social groups can be a building block for healthier bottom-up democratic renewal. This could help integrate, or at least mitigate, disaffected elements of society that give disinformation in an American context outsize influence.

3. Fact check in emergencies but prepare systematic approach for day-to-day resilience.[307] The heightened will surrounding Ukraine, for instance, has mostly unified Americans in rejecting Russian disinformation. Some right-wing media outlets have

305. DiResta, 2018.
306. Dew, 2019, p. 157.
307. Splidsboel, 2017, p. 19. "The active debunking of disinformation, via a meticulous de-construction of the news items, is advisable in extraordinary circumstances, such as the risk of heightened tension or even outbreak of conflict within a state or between states, as well as for educational purposes… It is not, however, to be considered a systemic response. For that it is too patchy."

continued pushing pro-Putin, pro-Kremlin narratives, but they are far outweighed by most of the coverage documenting the brutality of Russia's war. Right wing media is particularly vulnerable to disinformation because it is not motivated by accuracy, but by partisan interest.[308] The shock of the invasion will wear off, so while directly confronting disinformation now is important, long-term solutions must include educating Americans on how to recognize and critically assess disinformation.[309]

4. Recognize that nothing is inevitable. This corresponds to not overestimating or underestimating Russia. The United States Government and civil society should push Americans to take responsibility for their democracy. Democracy is under attack through subversion, but it is not defeated. Efforts to destroy democracy could go either way. The United States Intelligence Community's "Global Trends 2040" report argues that democratic decline is not preordained; democracy has been challenged before and could be reenergized in coming decades.[310] This is made less likely by politicians who question elections. These actors are advancing Russian objectives wittingly or not.[311] But renaissance is made more likely if citizens are encouraged to participate and take ownership in government at all levels.

In conclusion, the struggle between democracy and Kremlin disinformation will continue for the foreseeable future. Attacks will still emanate from Russia, but will also

308. Benkler et al., 2018, p. 8. The American right-wing media ecosystem makes public discourse "vulnerable to disinformation, propaganda, and just sheer bullshit."
309. Richey, 2018, p. 113.
310. National Intelligence Council, "Global Trends 2040: A More Contested World", 2021, p. 84. "In particular, some foreign actors are attempting to undermine public trust in elections, threatening the viability of democratic systems. Both internal and external actors are increasingly manipulating digital information and spreading disinformation to shape public views and achieve political objectives."
311. Snyder, 2021. "An elected institution that opposes elections is inviting its own overthrow. Members of Congress who sustained the president's lie, despite the available and unambiguous evidence, betrayed their constitutional mission."

be supported, amplified, or originated from right-wing parties across Europe and the United States. Predictable events like elections will remain targets. Unpredictable shocks like COVID and the Russian war in Ukraine will impact democratic will. The COVID pandemic has revealed that while events change, disinformation themes and tactics remain the same. The war in Ukraine has shown that democratic will may be higher than Russia anticipated, at least in the short term and in the face of shocking military aggression. The future trajectory of democracy will mostly depend on actions taken not during these exceptional crises, but during the less dramatic regular functions of boring, but essential time between crises. In that time, democracies must build and maintain the will to resist corrosive disinformation. Every time an attack weakens democracy, future responses become less sure. And it is always the long term which must be guarded. Snyder frames the stakes, especially for the United States:

> The lie outlasts the liar. The idea that Germany lost the First World War in 1918 because of a Jewish "stab in the back" was 15 years old when Hitler came to power. How will Trump's myth of victimhood function in American life 15 years from now? And to whose benefit?[312]

312. Snyder, 2021

APPENDIX A
INDIVDUAL COUNTRY SUMMARIES

Low Will, Low Capability (Poland, Spain)

Coorelates of War CINC			NCPI Ranking (Information Control and Norms)			OECD Trust		
	Avg. 2013-16	Since 1991	State	Average		State	Average	
United States	0.13204	Q1	United States	1.0	Q1	Netherlands	61.31	Q1
Russia	0.03786	Max .15630	United Kingdom	7.0		Germany	58.83	Max 80.86
Germany	0.01688	Q2 .01998	Russia	7.5		Canada	58.02	
United Kingdom	0.01433		France	10.0	Q2 9.4	Finland	57.01	
France	0.01374		Australia	11.0		Sweden	55.48	Q2 55.73
Italy	0.01150		Sweden	11.0		Russia	51.57	
Canada	0.00861	Median .01040	Canada	12.5		Australia	45.66	
Spain	0.00764	(Q3 .02281)	Netherlands	14.0	Q3 12.8	United Kingdom	40.42	Q3 44.92
Australia	0.00674		Germany	15.5		France	36.22	
Poland	0.00549		Spain	17.5	Q4 16.0	United States	35.09	
Netherlands	0.00398	Q4 .00543	Lithuania	22.5		Lithuania	33.86	Q4 34.52
Sweden	0.00210	min .00039	Italy	24.0		Poland	33.11	Min 14.57
Finland	0.00151					Spain	29.10	
Lithuania	0.00041					Italy	25.19	

Table 15: Ratings for Low Will, Low Capability States

			Expected Action		
Legend:			State inaction; do nothing	Poland	Spain
Observed	Low Will	Low Capability	Inchoate response by domestic sectors, limited to no role internationally	Poland	Spain
Inconsistent			Democratic backsliding: institutions weaken, reduction in domestic freedoms and rights	Poland	Spain
Not observed					

Table 16: Overall Findings for Low Will, Low Capability States

Poland

This former Soviet Republic was a state with great democratic promise at the end of the Cold War and into the new millennium. Its ruling party has since ignored external Russian threats in favor or employing disinformation domestically. Its democracy and institutions have weakened; however, it still participates in NATO disinformation efforts internationally.

Poland qualifies as low will and low capability. In each of the measures considered here, Poland ranks low among the set of chosen democracies. The state's average CINC of .00549 ranked 10 of 13 democracies. The Belfer Center did not include Poland in its

2020 NCPI rankings. However, considering that both of its closest neighbors in the sample for this project, Germany and Lithuania, have low component scores, and the fact that Poland is very close to Spain in other measures, it seems fair to assume that it would likely rank among the least capable quartile. Its Organization for Economic Cooperation and Development Trust rating also shows that Poland is in the lowest trust quartile with an average score of just under 33% population expressing trust in the government. All measures show that Poland is low capability and low trust. This does come as a surprise given Poland's history during the collapse of the Soviet Union.

Poland has a unique history in discussing Russian propaganda. At the time the Soviet Union collapsed, Poland was a satellite republic and a focal state that many expected would most fervently embrace democracy. Anne Applebaum, who has lived in Poland since the 1990s and whose husband has served as a Polish defense minister and foreign minister, has detailed the changes in the Polish Right over the past few decades. Many of her friends, once staunch pro-democracy conservatives, are now unrecognizable to her.[313] They have become zealous supporters of the Law and Justice party (PiS), which has turned the power of the state against democracy in Poland. Over the period I studied, Poland became more concerned with employing disinformation domestically than in countering disinformation stemming from Russia.[314] There, the expectations of a low capability, low will state were evident.

First, as the state did not do anything about Russian disinformation, Civil Society Organizations (CSO) did emerge to fill the void. Also, as expected, without the

313. Applebaum, Twilight of Democracy, 2020.
314. Gregor and Mlejnková, 2021.

centralized planning or control that a state could provide, the response has been scattershot. Project 'Demagog,' for instance is a CSO founded to fact check election debates.[315] Also, following the example of similar Ukrainian organizations, an ad hoc group 'Wojownicy Klawiatury' (Keyboard Fighters) emerged to push back against disinformation being spread about European Union elections while other organizations like StopFake, Rosyjska V kolumna w Polsce (Fifth Russian column in Poland), Disinfo Digest, and InfoOps Poland all sprouted to address Russian disinformation.[316] The efforts were not coordinated by the State, though, and were mostly modeled off of efforts in different countries. After Law and Justice consolidated power in the country, the growth in CSOs continued for a few years peaking in 2017 with the creation of 14 organizations to fight disinformation. But, by 2019, there were no new organizations created.[317] The government did eventually setup a counter disinformation effort in 2018, but it was aimed at debunking disinformation about procedures and ballots during the country's presidential election. The effort was a website called "Safe Elections" and did not do anything about the main problem of Russian influence in the country[318]. The lack of action taken by Law and Justice did not prevent them from having to deal with the fallout from Russian operations. The government responded in 2020 to a false story that the Polish counterintelligence service kidnapped a Lithuanian soldier for spying.[319] Ignoring the external threat of Russian disinformation in favor of focusing on internal domestic control did not make the external threat go away. The Russian threat remained persistent.

315. Gregor and Mlejnková, 2021.
316. Gregor and Mlejnková, 2021.
317. Gregor and Mlejnková, 2021.
318. Jankowicz, 2020.
319. Polish Government, 2020.

Law and Justice's choices over the period clearly weakened democracy in Poland, advancing Russian goals at the cost of Poland.

Second, Law and Justice has employed disinformation domestically, seeking to consolidate power. At the same time, wittingly or not, they have been leaving the country exposed to Russian disinformation seeking to undermine democracy. This has resulted in weakening institutions and curtailed domestic freedoms, especially around press freedom. After taking power in 2015, the party took control of publicly funded radio and television networks. The outlets were set up to be neutral outlets, but Law and Justice began using them as means to propagate party-friendly messaging. Any journalists who refused to stick to the party line were fired.[320] The television network fired at least 235 journalists and has increasingly become an outlet that Law and Justice uses to employ the tools and tactics of disinformation domestically.[321] Law and Justice has also employed bot networks, troll farms, and other inauthentic digital disinformation tactics also employed by Russian agencies to influence elections and pressure those who deviate from party messaging.[322] After turning the state networks into propaganda outlets, Law and Justice even went so far as to install a loyalist chairman over the protest of Poland's National Media Council (oversight board) and increased the networks' budget substantially. The network used some of the money to track political opponents and spy on journalists.[323] Since Law and Justice took power, Poland has fallen down the list of Reporters Without Borders' World Press Freedom Index. In 2015 Poland was ranked 18. Poland in 2020

320. Kosc, 2020.
321. Jankowicz, 2020.
322. Jankowicz, 2020.
323. Kalan, 2019.

slipped to 62 of 180 ranked countries.[324] Law and Justice has not only looked the other way regarding Russian disinformation but has also tried to employ the same disinformation tools and tactics as a means of domestic control. This has hastened a decline in democracy within a former Soviet satellite republic with the effect of advancing Russia's goals of undermining democracy globally and especially in states close to its borders.

Spain

Spain exhibited all expected responses to Russian disinformation for much of 2013-2020. The state did begin taking stronger actions later in the period following Russian interference in the 2017 Catalan secession vote. Since then, Spain has been alerted to Russian election interference and medical disinformation early in the COVID pandemic.

Spain scores very similar to Poland in the measured aspects of will and capability. It is low in both. Its average CINC score was .00764 only slightly below average for the democracies. However, the average score for its Information Control and Norms scores in the Belfer Center's NCPI rankings put it in the least capable quartile. And only Italy scored lower for average trust score in the Organization for Economic Cooperation and Development surveys.

The Spanish government was not a leader in the period considered for this work but emerged in the later years to take Russian disinformation more seriously. I found little discussion of Russian disinformation in Spain from 2013-2017 and little evidence that the Spanish government was doing much to combat it. However, 2017 was a turning point. In

324. Kosc, 2020.

that year, there was a vote for Catalonia to secede from Spain. Sowing such internal divisions would be a natural fissure that Russian influence would seek to exacerbate. The Spanish government had not addressed the Russian threat directly until then, but at the highest level publicly accused Russia that year for interference with elections. The Prime Minister accused Russia in meddling in the European elections[325] and the Foreign Minister stated, "I am going to put it on the record that in other areas [such as Catalonia], not only in the community to our East, situations of manipulation and disinformation are arising."[326] As a result, Spain updated its national security strategy to include the threat of misinformation campaigns. Spain did not name Russia directly in the strategy, but the document is evidence that the threat in Spain was becoming clearer to the government, especially considered in context of the Prime Minister's and the Foreign Minister's statements.[327] Spain, then, conforms to some of my predictions, but not all.

First, early in the period I considered, Spain appears to have not been doing much about the Russian threat. This could be because they were focused on countering different threats. Spain has been fighting Islamic extremists and terrorists within Spain. As a state with limited capability, it likely put its focus against immediate threats. However, Spain did realize the threat from Russia in and around 2017. Even in European Union-wide, and NATO-wide papers, Spain is rarely mentioned except that they've been a target of attacks. This could indicate that they are just supporting European Union and NATO collaborative efforts as an alternative to taking a state-level response. This is not what I

325. Booth and Birnbaum, 2017.
326. Spain Claims Russian Meddling in Catalan Crisis, 2017.
327. Jopling, 2018.

would expect for a low will state. This would make sense for a low will state which comes to realize the threat late. The 2017 Catalan vote to secede prompted a strong reaction from Spain's national government which resulted in jail time for opposition politicians and dissolving of the Catalan government in favor of direct rule from Madrid.[328] This is certainly a reduction in rights for citizens and a major crisis precipitated within a NATO ally. The articles and sources did not evidence CSOs in Spain targeting Russian attacks. Spain is a mixed case for my theory from 2013-2020; less serious about the Russian threat in 2013 than 2020, but Spain whatever change in the seriousness with which Spain viewed disinformation in the period I covered would intensify with the COVID pandemic. Spain was an early epicenter from disinformation about the disease, its causes, and vaccine disinformation. This likely focused the government's perception of the threat from disinformation and is worthy of further exploration.

Low Will, High Capability (Italy, United States)

Coorelates of War CINC			NCPI Ranking (Information Control and Norms)			OECD TrUnited Statest		
	Avg. 2013-16	Since 1991	State	Average		State	Average	
United States	0.13204	Q1	United States	1.0	Q1	Netherlands	61.31	Q1
Russia	0.03786	Max .15630	United Kingdom	7.0		Germany	58.83	Max 80.86
Germany	0.01688	Q2 .01998	Russia	7.5		Canada	58.02	
United Kingdom	0.01433		France	10.0	Q2 9.4	Finland	57.01	
France	0.01374		Australia	11.0		Sweden	55.48	Q2 55.73
Italy	0.01150		Sweden	11.0		Russia	51.57	
Canada	0.00861	Median .0104	Canada	12.5		Australia	45.66	
Spain	0.00764	(Q3 .02281)	Netherlands	14.0	Q3 12.8	United Kingdom	40.42	Q3 44.92
Australia	0.00674		Germany	15.5		France	36.22	
Poland	0.00549		Spain	17.5	Q4 16.0	United States	35.09	
Netherlands	0.00398	Q4 .00543	Lithuania	22.5		Lithuania	33.86	Q4 34.52
Sweden	0.00210	min .00039	Italy	24.0		Poland	33.11	Min 14.57
Finland	0.00151					Spain	29.10	
Lithuania	0.00041					Italy	25.19	

Table 17: Ratings for Low Will, High Capability States

328. Minder, 2019.

			Expected Action		
Legend:	Low Will	High Capability	Weakened or no state reaction against external threat	Italy	USA
Observed			Employment of state capability to use disinformation tactics against domestic audiences	Italy	USA
Inconsistent			Democratic backsliding: broken trust, institutions weaken, reduction in domestic freedoms and rights	Italy	USA
Not observed			Social division and struggle between domestic sectors, balance of power determines future direction.	Italy	USA

Table 18: Overall Findings for Low Will, High Capability States

Italy

Italy displayed all expected responses for a low will high capability state. It has a history of sympathy and support for Russia, it ignored and sometimes actively amplified Russian disinformation domestically, and it took all the way to 2020 for the Italian government to begin addressing the Russian threat.

Italy is the clearest example in this study's sample of a low will high capability state. By the average of 2013-3016 Correlates of War CINC score, it ranks fifth most capable. However, despite its aggregate strength, its specific capabilities that could facilitate an effective response to Russian disinformation rank lowest among all states in the sample. Not only is Italy lowest for its Information Control and Norms scores according to the Belfer NCPI, but it also scores lowest in average trust. On average from 2012 to 2020 Organization for Economic Cooperation and Development surveys, just 25% of Italians expressed trust in their government. Italy's average was lowest, and it also scored the lowest individual record of all state years for the period. In the 2013 Organization for Economic Cooperation and Development survey, only 14.6% of Italians said they trusted their governments. These scores place Italy in the low will high capability quadrant; it is a powerful state which did not mobilize to face the threat of Russian disinformation. Its

unique history and relationship with Russia help explain their lack of state will to push back and its policy choices reflect expected outcomes.

Among the sample of states, the Italian government has a unique history with the Soviet Union and with Russia among the sample. Throughout the Cold War, Italy had a large Communist party.[329] This resulted in more sympathy for the USSR than existed in many other states. During the Cold War and since, Italy has been one of Russia's best European partners. Early in 2020, this trend was evidenced in a nationwide poll where Italians indicated more favorable views of China and Russia as a "friend" of Italy than they did for the United States. China scored 52%, Russia was 32%, and only 17% expressed a positive view of the United States.[330] Andrew Weiss argued that this outcome stems from Italy's actual and perceived distance from the threat:

> Countries closer to Russia's borders, who spent much of the twentieth century under the Soviet yoke, often view Russia as a dissatisfied power with lingering imperial ambitions that must be confronted and contained. Moving west, European states grow more relaxed on the Russia question, with political leaders open to mollifying Russian insecurity with a tighter political and economic embrace and wary about the post-2014 direction of United States Policy.[331]

Its size, history, geography, and relative sympathy with Russia made Italy late to understand the threat of disinformation, but ignoring the threat is not an effective policy for mitigating its harms. Later in the 2013-2020 period, the Italian government did start recognizing the threat. Its choices fit the expected steps of a low will high capability state.

329. Weiss, 2020.
330. Christiani, 2020.
331. Weiss, 2020.

Italy's response to Russian disinformation was weak to none early in the period, national politicians used Russian propaganda domestically, and the impacts show in Italy's broken trust. In late 2016, the Italian Prime Minister directly asked Russian President Vladimir Putin about Russian propaganda ahead of an Italian constitutional referendum.[332] Soon thereafter, Italy established its own Joint Command for Cyberspace Operations.[333] Although Italy was a sponsor state for NATO's Strategic Communications Center of Excellence in Riga, Latvia, Italy did not engage seriously in its mission to combat disinformation.[334] The Italian government did create an online reporting system for citizens to report fake news to police[335], but some of the country's prominent politicians, including the Deputy Prime Minister spread fake news and pro-Putin disinformation even using for his official campaign website the same propagandist who built other websites like "I'm with Putin," and "StopEURO.[336] The mid-2010s domestic use of disinformation campaigns used by Deputy Prime Minister Salvini and other far-right Five Star Movement politicians did start to raise the issue of disinformation among priorities in the Italian body politic, but Five Star politicians remained in the governing coalition through the end of the period covered in this dissertation. Italy, being a natural Mediterranean crossing point from North Africa was more focused on immigration and Islamic propaganda than pushing back on Russian disinformation.[337] Of course, Russian attacks served to highlight these issues to further undermine already low Italian trust in

332. Weiss, 2020.
333. Kremlinwatch.eu, 2021.
334. Kremlinwatch.eu, 2021.
335. Gregor and Mlejnková, 2021.
336. Appuzo and Satariano, 2019.
337. KremlinWatch.eu, 2021.

democracy. The lack of state focus did lead to some other sectors trying to tackle the problem. Several civil society organizations formed around the issue, but Italy has no legal, institutional, or policy frameworks for educating its people on the Russian threat.[338] Finally, in 2020, the Italian government publicly named Russia and China for spreading disinformation in Italy and released previously classified intelligence to support the accusation.[339]

The actions undertaken by the Italian government were not those required by powerful democracy to protect itself from the Russian threat. Italy's response has been weak and slow, its politicians have used disinformation and Russian propaganda domestically, and the already low trust that Italians had in their country continues to poll at the weakest levels of any state in the sample states. All of this is consistent with a high capability state that lacks the will to confront disinformation.

United States

The United States Government responses were mixed for 2013-2020. No other state was the target of so many Russian operations than the United States. Its high rankings for capability are the result of counter-Islamic State successes early in the period. After the 2016 election, parts of the government acted against Russia, but the response was hampered without Presidential leadership. One of the two major American parties has embraced disinformation as a tool for maintaining power domestically.

The United States from 2013-2020 was by far the world's most powerful democratic state and, by extension, the biggest target of Russian disinformation operations. In fact, of

338. KremlinWatch.eu, 2021.
339. Christiani, 2020, and Bechis, 2020.

the states in my sample, only five states were targeted multiple times by publicly identified Russian influence campaigns. The Netherlands, Germany, and Australia were targeted twice, the United Kingdom was targeted three times, and the United States was the target in fourteen such attacks.[340] The United States is targeted so often because it is rife with sharp internal divisions and because undermining the United States also undermines the United States-led rules based postwar global order. The Correlates of War CINC average for the United States from 2013-2016 was greater than the combined total of all other democracies in the sample plus Russia. The United States also topped the Belfer Center's ratings for information control and norms components of their cyberpower rankings. It is, therefore, clearly a high capability state. With regards to trust among its people, the United States Government averaged 35% trust among its population. That scored ninth worst of thirteen— just less France and just higher Lithuania. The United States is also considered a "flawed democracy" according to the Economist Intelligence Unit's 2020 ratings and has been trending lower in its democracy score in recent years. The disparity between its capability, and its democratic will is widening. The United States did not conform fully to expectations of a high capability low will state, but I believe that is because the government is in the midst of change which will either see it restore its will to resist disinformation or continue to act in ways which will precipitate further democratic decline.

The first expected response by a high capability low will state is weak to no action against an external threat. Here, the results were mixed. The United States did take

340. Martin et al., 2020.

actions against Russia. President Obama and Congress created a Global Engagement Center in December 2016 to combat Islamic State and Russian propaganda.[341] Admiral Rogers, as Director of the National Security Agency, attributed electoral interference to Russia during the 2017 French Presidential election. The National Security Agency shared this attribution with France, helping France take the proactive steps it did to mitigate the harm.[342] The government launched multiple investigations into Russian interference including Intelligence Community Assessments, House and Senate committee investigations, and the Special Counsel investigation led by Robert Mueller.[343] The Mueller investigation itself resulted in dozens of indictments both of Americans, Russian organizations, and Russian military officers.[344] Still, these efforts were weakened by elected Republicans, President Trump, and officials in the Trump administration. When President Obama brought evidence of Russian interference to Congressional leaders, Majority Leader McConnell politicized a decision to make public the information before the 2016 election. Once elected in the most successful, from a Russian perspective, attack on democratic politics,[345] President Trump refused to acknowledge the threat and took every opportunity to undercut efforts at addressing it. So, while the government did take serious actions to combat Russian disinformation, those efforts were also weakened by the leader of the government. This is a mixed result.

The second and third expectations of a high capability low will government were evident. The President and Trump administration officials used their influence and White

341. Stengel, 2019.
342. Nance and Reiner, 2018, and Davis, 2018.
343. Davis, 2018.
344. Jopling, 2018.
345. Jopling, 2018.

House positions to become the largest node in a network of right-wing disinformation outlets.[346] The President and others used their positions to lie at an unprecedented scale and rate throughout his campaign, administration, his ultimately unsuccessful 2020 bid for reelection. The National Intelligence Council released an unclassified retroactive report on the 2020 election which highlighted foreign threats to that 2020 election. Despite the United States President's denials and false claims, the report highlights the threat of disinformation and is mostly about Russia.[347] Instead of having a government led by an official defending American interests, instead the administration was undermining institutions and trust. It used disinformation as a technique to build and maintain power then used that power to facilitate a systematic effort to erect barriers to opposition voters and even ended up organizing an attack on the Congressional certification of his defeat. The United States' democracy entered this period with significant issues in its democracy, but throughout the period disinformation became central to a Presidential administration and one of two major political parties. By 2020, that democracy continued to decline, and the country even began experiencing unprecedented political violence based on lies. This is consistent with expectations for a low will high capability state.

The last expectation for low will high capability response is social division, struggle between domestic sectors, and that the balance of power determines the state's future direction. This expectation was evident. Where the government failed to act, others stepped in. Campaigns, now operating in an environment where disinformation is

346. Benkler, 2018.
347. Applebaum, 2021.

increasingly utilized by Americans against Americans, hire expensive cyber and information experts to help navigate threats.[348] This raises the cost for participating in politics and increases the threshold that candidates must clear just to compete for office, further undermining democratic participation. The Atlantic Council Digital Forensics Lab stepped up to fill a void where the United States Government might typically be expected to contribute. It is an effort to expose and counter disinformation as a means of combatting Russian hybrid attacks against democracy.[349] In September 2017, the Department of Homeland Security informed 21 states that Russia had attempted to access their state voter databases.[350] Officials from the Obama administration and even the early Trump administration including Secretaries of State and Ambassadors to the United Nations noted the uptick in Russian "hybrid warfare" operations around the world.[351] A veto proof majority in the then-republican controlled Senate imposed increased sanctions on Russia ahead of the 2018 midterms.[352] Again, anywhere President Trump held sway, these efforts were minimized, opposed, and silenced. His power in the party only grew over time and the degree to which he or other similar-minded leaders control levers of power, the United States will turn away from confronting external disinformation with the considerable capabilities it possesses. Rather, the fight will turn inwards as a struggle between competing domestic constituencies competing against each other while all Americans remain under attack from Russian state disinformation.

348. Davis, 2018.
349. Hanzelka and Pavlikova, 2021.
350. Davis, 2018.
351. Hall, 2017, and Jopling, 2018.
352. Jopling, 2018.

The United States' response to Russian disinformation from 2013-2020 was mixed. Early in the period, the threat was not as apparent as it should have been. The 2016 election was a spectacular failure which ushered in political leadership that campaigned then governed using disinformation. As a result, American democracy declined and faces critical years ahead. If it uses its capabilities to fight disinformation, it can improve its democratic health. If its leaders continue to employ disinformation domestically, all Americans will suffer and the United States-led global order will face increasing challenges.

High Will, Low Capability (Australia, Finland, Lithuania, Netherlands, Sweden)

Coorelates of War CINC			NCPI Ranking (Information Control and Norms)			OECD Trust		
	Avg. 2013-16	Since 1991	State	Average		State	Average	
United States	0.13204	Q1	United States	1.0	Q1	Netherlands	61.31	Q1
Russia	0.03786	Max .15630	United Kingdom	7.0		Germany	58.83	Max 80.86
Germany	0.01688	Q2 .01998	Russia	7.5		Canada	58.02	
United Kingdom	0.01433		France	10.0	Q2 9.4	Finland	57.01	
France	0.01374		Australia	11.0		Sweden	55.48	Q2 55.73
Italy	0.01150		Sweden	11.0		Russia	51.57	
Canada	0.00861	Median .01040	Canada	12.5		Australia	45.66	
Spain	0.00764	(Q3 .02281)	Netherlands	14.0	Q3 12.8	United Kingdom	40.42	Q3 44.92
Australia	0.00674		Germany	15.5		France	36.22	
Poland	0.00549		Spain	17.5	Q4 16.0	United States	35.09	
Netherlands	0.00398	Q4 .00543	Lithuania	22.5		Lithuania	33.86	Q4 34.52
Sweden	0.00210	min .00039	Italy	24.0		Poland	33.11	Min 14.57
Finland	0.00151					Spain	29.10	
Lithuania	0.00041					Italy	25.19	

Table 19: Ratings for High Will, Low Capability States

			Expected Action	
Legend:	High Will	Low Capability	State employs indirect (defensive) efforts. Ex: defense alliances, multinational institutions, public education	Australia Finland Lithuania Netherlands Sweden
Observed			Protect democratic institutions/processes domestically	Australia Finland Lithuania Netherlands Sweden
Inconsistent			Build resiliency domestically	Australia Finland Lithuania Netherlands Sweden
Not observed			Integration among domestic sectors: government, media, society	Australia Finland Lithuania Netherlands Sweden

Table 20: Overall Findings for High Will, Low Capability States

Australia

Australia has responded to protect norms and build resiliency domestically. It has focused its efforts on elections and education at home. It also has been very active

supporting international efforts against Russian disinformation, likely anticipating China's increase adoption of aggressive Russian disinformation tactics.

Australia is a border case when considering capability, but its government has clearly demonstrated a high will to confront disinformation. The country's average Correlates or War CINC score of .00674 is below average. That measure puts it between Spain and Poland in the third quartile. However, Australia's rankings were high in the Belfer scores for the disinformation-relevant components of the NCPI. Australia is higher in the second quartile for those measures. This means that while Australia may not have the overall capability of the powerful democratic states in the sample, it is specifically capable in ways that matter to combatting disinformation. Further, the Australian government has shown a will to act and enjoys comparatively high trust among its people. Australia's average Organization for Economic Cooperation and Development rating was roughly 46% from 2012 to 2013 which was higher than average for the selected democracies. That trust may reflect the Australian Government's demonstrated will in acting along all expected techniques for a low capability, high will democracy.

The Australian has employed defensive efforts against disinformation, built resiliency domestically, and integrated actions across domestic sectors of society. Defensively, the government took several actions to educate its public. The government created a foreign influence register that requires disclosure statements by anyone working for a foreign principal to influence Australian political outcomes. And, in 2019, Australia started a "Stop and Consider" campaign to help voters think through and evaluate the veracity of

their sources of information.[353] The government also took actions to bolster its internal democratic institutions, especially elections. Australia created an Electoral Assurance Taskforce in 2018. It banned foreign funding for political advertisements, requires all paid electoral advertisements be authorized and identified with an authorization statement.[354] In addition, the government has made criminal the attempt by foreigners to interfere in governmental processes, domestic exercise of political rights, or undermining national security. Australia is also a part of the Christchurch Call, an international effort to combat extremism online. "Abhorrent violent material" can be removed from the internet under Australian law and the government has explicitly tied this language to disinformation. The electoral commission worked with major social media platforms like Facebook and Twitter to develop ways of blocking communications that violate these laws.[355] These efforts to educate, protect democracy domestically, and integrate separate sectors are largely aligned with expectations for what a high will low capability democracy would do to counter the threat from disinformation.

Following the years covered in this survey, there has been an accelerated effort from the Australian government to push back against disinformation. The changes in Australian law escalated conflict with Facebook. Additionally, the government has continued to pursue a balancing strategy in the Pacific. Although it appears China is the major threat from Australia's perspective, still they have banded together with other democratic states in pushing back against authoritarianism in the region. Just as Poland's

353. Levush, 2019.
354. Levush, 2019.
355. Levush, 2019.

inaction against the Russian threat wittingly or unwittingly advances Russian interests, pro-democracy efforts like Australia's still counter Russian malign objectives.

Finland

Finland has a long history of opposing its much more powerful neighbor. The threat from Russia is sustained and existential. Finland's government, then, has been a leader in pushing back against Russian disinformation participating and building domestic resilience, supporting multinational efforts, and cultivating a comprehensive societal response. Its government has the highest trust among its people and that trust increased during the period.

If Australia is a border case for consideration as high will low capability, Finland epitomizes the category. Finland's CINC score ranks it as the second least capable democracy of the selected states. The Belfer Center NCPI does not even include Finland in their sample. If the NCPI had included Finland, it is likely that the Finland would have been somewhere in the middle of the pack. Finland, according to its existential interests, has over the past decades balanced stout defense domestically against Russian influence with keeping a lower profile internationally. This is a way to stay sovereign without unnecessarily provoking their much more powerful neighbor to the East. As such, I expect that Finland would get high marks for "Information Control" since it has been able to fend off Russian disinformation, but lower marks for "Norms" since it has achieved its information control quietly. This would rank them close to Sweden— which, given their similar approach and direct cooperation, seems reasonable. Regarding Organization for Economic Cooperation and Development Trust, Finland is in the top quartile for average

annual trust ratings among its citizens. Within that high average, however, two trends make it even more impressive. First, Finland's trust has generally increased from 2012-2020. And second the states measured each year since 2012, Finland had the highest single-year rating of 81% trust in the most recent year measured. So, Finland is the example of high will low capability; it is a tiny state next to a huge power and united in its will to stay independent.

Just as Finland's clearly high will and low capability, its governmental actions are very much in line with expected behaviors. It has employed defensive measures, protected institutions domestically, built resiliency, and integrated sectors of society to combat disinformation.

Finland has employed defensive measures including bolstering multinational institutions, public education, and defense alliances. Helsinki is host to the European Centre of Excellence for Countering Hybrid Threats, which has been operating since 2017.[356] The government has focused on working through the European Union for regulation and actions against digital platforms. Finland recognizes that the European Union's market power and regulatory capability is much more likely to result in changes than Finland could hope to achieve alone.[357] And Finland has worked with other partner states bilaterally or through defense alliances even as a non-allied state. In 2016, Finland and Sweden jointly condemned Russian propaganda in the region.[358] Finland has worked with United States experts to train Finnish officials responding to fake news and has

356. Splidsboel, 2017, and Tiido, 2019.
357. Schia and Gjesvik, 2020.
358. Pynnöniemi, 2019.

confirmed support for sanctions against Russia for attacking Ukraine.[359] Finally, Finland is a member of the NATO Strategic Communications Center of Excellence. It participates in this multinational effort even though it is not a NATO member state.[360] Finland works with anyone who will work with it to push back against Russia: regional neighbors, European Union members, NATO, and the United States. It also works domestically to build resiliency.

The government has protected domestic institutions and built resiliency at home. The Finnish intelligence service has identified dozens of recent Russian information operations.[361] In March 2019, the Finnish government passed a law that requests candidates for security postings to prove they do not have dual loyalties to other nations or beliefs that might undermine national security.[362] Education campaigns have included training for government officials and the public. Government officials and political parties are trained on the science of disinformation, including emphasizing the need to advance a positive "Finnish story" that highlights national values.[363] The government also aimed campaigns at educating its people. Since the 1960's Finland has recognized the security implications of Soviet, now Russian, propaganda and has emphasized media and information literacy as a "civic competence."[364] The government has supported this goal in school curricula and in media campaigns. Critical reading of the news is taught in schools.[365] Prominent national celebrity personalities and officials publicly bolstered the

359. Pynnöniemi, 2019.
360. Hanzelka and Pavlikova, 2021.
361. Pynnöniemi, 2019.
362. Tiido, 2019.
363. Hanzelka and Pavlikova, 2021.
364. Jankowicz, 2018.
365. Haciyakupoglu, et al., 2018.

security and reliability of the electoral system leading up to elections in 2019.[366] This strategy of education, along with cultivating trust in the government, has been successful. The Finnish-language version of Sputnik closed because not enough people read it.[367] Finland's government has employed an effective strategy against Russian disinformation by bolstering its institutions and inculcating resiliency among its people. It has made those efforts more effective by linking actions across sectors.

Finland has integrated efforts among various sectors of its society including leaders from media, government, military, and culture. The Finnish national broadcast network does reporting in Russian. This not only reaches Russian-speaking Finns, but also achieves influence across the border into Russia.[368] Government also integrates many different leaders and stakeholders in developing its policies regarding media literacy. These include leaders from Ministries of Education and Culture, Justice, Culture and Sport, and others.[369] Because the Finnish government has educated leaders across sectors on the social science underpinning tactics of disinformation, each contributes to pushing back against it.[370] As mentioned, celebrities and public officials have supported electoral integrity media campaigns. But the collective understanding that Russian disinformation is a threat also impacts media coverage of Russian narratives. Main outlets were critical of Russian narratives leading up to their invasion of Ukraine, for instance, in ways that

366. Schia and Gjesvik, 2020.
367. Jopling, 2018, and Schia and Gjesvik, 2020.
368. Tiido, 2019.
369. Jannkowicz, 2018.
370. Jankowicz, 2018.

contrasted with media in other countries which have journalistic norms which allow propaganda to amplify.[371]

Finland is a clear case of high will and low capability. They are one of the least powerful states among the chosen set of democracies in this work, yet perhaps because of that, have used all tools at their disposal quite effectively to inoculate the country against Russian disinformation.

Lithuania

Lithuania is a tiny former Soviet Republic which is highly attuned to the threat of Russian disinformation. Russian aggression is an existential threat to Lithuania, which has driven its government's emphasis on joining and enthusiastically supporting NATO. Lithuania has Finland's will to resist, but its government is a young democracy without the same support trust of its people. The government promotes resiliency, but the strongest actions have come from its people, banding together in ad-hoc groups of "elves" who fight disinformation.

Lithuania is also a clear case of a high will low capability state. It is the only state lower than Finland in its average CINC score for 2013-2016, at a minuscule .00041. This is less than a third of Finland's already modest score. So, Lithuania is tiny. It also ranked low among the Belfer Center's ratings for Information Control and Norms in the NCPI rankings. Only one other country ranked lower when averaging the two category scores. Regarding trust, Lithuania is the opposite of Finland. Where Finland is among the most trusted government according to its people, the Lithuanian government had an average

371. Pynnöniemi, 2019.

Organization for Economic Cooperation and Development Trust rating of 34%. That is in the lowest quartile of the selected democracies. Finland and Lithuania have very different histories with the Soviet Union which likely drive such a divergent result in trust. While Finland fought against the Soviets and was able to remain sovereign, Lithuania was a part of the Soviet Union until its dissolution at the end of the Cold War. Despite its meager capabilities, the government has demonstrated high will to fight disinformation. Its actions fit those expected of a high will low capability state.

Defensive efforts taken by the Lithuanian government are consistent with predictions for a high will low capability state. The government has sought to leverage alliances, multinational institutions, and total defense doctrines. For example, it signed on with other countries in the region to create a Baltic Cultural Fund. The fund encourages ties between states and promotes military, media, and cultural groups working together.[372] Lithuania, in addition to being a member of NATO, is part of the Nordic-Baltic 8 (NB-8) regional defense framework.[373] These states includes NATO members and non-NATO members, all near their much more powerful neighbor, Russia. Lithuania coordinated founding in 2018 the European Union's Cyber Rapid Response Teams.[374] And Lithuania has been a strong advocate for elevating Russian disinformation in the policy agenda within its borders and among the various multinational organization in which it participates. The Lithuanian government has pursued a strategy of leveraging multinational organizations as a defensive effort. These are formal and informal, military,

372. Financial Times, 2020.
373. Flanagan et al., 2019.
374. Sramkova, 2019.

cultural, and governmental arrangements designed to prevent them from falling into the hands of Russian aggression like has happened so many times along Russia's borders since 2008. Besides leveraging international partners, the government has also promoted resiliency at home.

In accordance with predictions for a high will low capability state, the Lithuanian government has acted to bolster its domestic institutions and to educate its people. The government has used temporary bans on Russian media found to be in violation of broadcast laws. Lithuanian law states that 90 percent of content on television in Lithuania must be produced in the European Union using official languages of the European Union. Broadcasters must translate into Lithuanian content longer than 90 minutes in a language not recognized as a formal European Union language.[375] Russian is not an official language of the European Union and must be translated. Further, even without securing a court order the government can shut down for up to 48 hours communication nodes or outlets propagating a disinformation attack.[376] These laws are meant to limit Russian disinformation from appearing in Lithuania or to provide ways to stop disinformation from spreading through broadcast media. The government has also pushed for its people to take responsibility defending against Russian invasion which increasingly has a strong component of weaponized disinformation. Even before Russia used these tactics invading Ukraine, Lithuania has advocated through public education like its "Guide to Active Resistance" for all citizens' responsibility for Total Defense resisting aggression however

375. Thomas, 2020.
376. Financial Times, 2019.

possible even to the individual level.[377] Lastly, the government has also pushed back against disinformation and publicly corrected the record in cases that threatened to drive wedges between it and its international partners. The state prosecutor debunked a story that alleged a rape by German forces in Lithuania during a NATO mission. The speaker of the Lithuanian government gave regular updates during the investigation to inform the Lithuanian public and to communicate to a broader NATO audience that the story was fake.[378] The Lithuanian government has demonstrated a high will to prevent Russian disinformation from impacting its population or threatening its partnerships. As expected, it also stresses integration among its social sectors.

In Lithuania, the government has made efforts to integrate efforts among various segments of its society and there is a prominent example of success. The civilian sector is very active in pushing back against Russian disinformation in real time. Lithuanian "Elves" act as a volunteer fact checking effort which is hosted and coordinated at a central website demaskuok.lt.[379] The elves themselves are an adhoc group of academics, journalists, scientists, and military members who collaborate using technology created by a Vilnius media group.[380] The website uses increasingly sophisticated software[381] to identify false narratives and has been so successful in Lithuania that a charity has expanded the effort to a website Debunk.eu, which coordinates with partners in multiple other countries as well. The Lithuanian elves are a demonstration of the state's leadership role in elevating disinformation on the international agenda. Further, the elves that

377. Flanagan et al., 2019.
378. Thomas, 2020.
379. Economist, 2019.
380. Financial Times, 2020.
381. Deutsche Welle, 2018.

operate through the site do so individually and collectively. This is consistent with the Total Defense resistance doctrine. Lithuania is the smallest country of the selected democracies. It punches above its weight in countering Russian disinformation, however, and the government acts in line with predictions for a low capability high will state.

Netherlands

The Dutch Government was very active during this period and showed a model for demanding Russian accountability for disinformation. Following the shootdown of nearly 200 Dutch citizens over Ukraine, the Dutch Government methodically proved Russian culpability and sustained a campaign pushing back against the flood of false Russian narratives surrounding the attack. The Dutch have also acted to protect their elections and rule of law at home.

The Netherlands is a state in the high will low capability category which has been very specifically motivated in confronting Russian disinformation in and surrounding its invasion of Ukraine. Russian forces killed hundreds of Dutch citizens in downing an airliner over Ukraine, prompting their government to seek accountability in the face of a flood of disinformation. By the numbers, the Netherlands is a small state with less capability than most of the other democracies in the sample. Its average CINC score from 2013-16 was .00398. This ranks in the least capable quartile. Dutch capabilities for the disinformation-relevant cyber capabilities were higher, but the Netherlands still ranked below average in the Belfer NCPI ratings for information control and norms. The country stands out, however, in its average Organization for Economic Cooperation and Development trust rating. From 2012-2020, the Netherlands had the highest average trust

rating of any democratic state in this study. 61% of Dutch citizens expressed confidence in their government over the period. This is well above the average of 45% for the entire sample and more than double the average trust in several of the distrustful states. The Dutch government's course of action in pushing back against Russian disinformation has followed expectations for a high will, low capability state.

The Dutch government has employed several defensive measures against Russian disinformation. First, it has joined on to multinational organizations dedicated to combatting Russian malign influence. The Netherlands joined the NATO Strategic Communications Centre of Excellence (StratCom CoE) in 2016. Only the nations who founded the Center of Excellence joined earlier.[382] The government has also employed public education campaigns and specifically named Russia as manipulative threat. Ahead of European Parliamentary elections, the Dutch government launched a public awareness campaign highlighting past cases of Russian meddling in other states' elections and warning Dutch citizens about the harms of disinformation.[383] And, the expert Dutch General Intelligence and Security Service (AVID) in its 2018 annual report directly named Russia's efforts to covertly interfere with elections.[384] These efforts are defensive efforts taken by an asymmetrically weaker state against a perceived threat from a more powerful actor. The Dutch government have not tried to punish Russia or compel it to do anything, but it has acted in concert with other states to push back against disinformation

382. https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5
383. Davis, 2018.
384. Hanzelka and Pavlikova, 2021.

and it has raised awareness domestically and internationally about the threat. The government has also taken actions to defend domestic institutions.

The Dutch government has pursued actions that protect domestic institutions and build resiliency within its population. First, although the Netherlands understood that it did not have sufficient capability on its own to confront Russia over the downing of a commercial airliner over Ukraine, it acted in a way to bolster facts and evidence in the face of a Russian campaign to obfuscate what had happened. For instance, it was the Dutch Safety Board that found Russia responsible for downing the airliner. The investigation was painstaking and time consuming but concluded that in 2014 Russian forces killed nearly 200 Dutch noncombatants.[385] The Dutch continued pressuring Russia in multiple fora to take accountability for their actions.[386] From the moment Russian forces shot down the commercial airliner over Ukraine, it rolled the incident into its information operations surrounding the invasion and the annexation of Crimea. The Dutch pushed back with facts and investigation, favoring truth over disinformation. The government also sought to protect the key democratic institution of elections. In 2017, the Dutch interior minister publicly stated that the Netherlands would be hand counted to prevent manipulation. This statement was actually a restatement; the Netherlands banned electronic voting ten years earlier in 2007.[387] Restating a policy was unnecessary, but the government was acting to bolster faith in elections responding to recent Russian influence

385. Higgins, 2017.
386. Golovchenko, et al., 2018.
387. Davis, 2018.

efforts. The Dutch have also integrated different sectors of society to fight disinformation.

The Dutch government in recent years has codified new responsibilities around disinformation and civil society organizations have also acted to stem the influence of false information. The government assigned new duties and responsibilities in 2019 to the National Coordinator for Security and Counterterrorism. The responsibilities include detecting foreign state influence operations.[388] Clarifying responsibility within government is important to gaining unity of effort; as the axiom goes, when everyone is responsible, nobody is responsible. The Dutch have recognized the threat from Russian disinformation and expressly put it in the purview of a specific governmental organization. Civil society has also responded to threats to the information domain. Dutch newspaper articles have fact check capabilities on social media outlets in the country.[389] Responses like these are those that this study's framework anticipate from states with low capability, but high will. These states, like the Netherlands, will use what capabilities they do have in concert with other states, in a mostly defensive manner, and in a more integrated approach spanning different social sectors.

Sweden

Sweden's Government has acted similarly, and in concert with, the Finnish Government. It has a comparably long history and experience of Soviet interference in its domestic politics, so the threat from Russia is different but not new. The Swedish Government has protected its domestic institutions and built resiliency while investing in

388. Hanzelka and Pavlikova, 2021.
389. Davis, 2018.

layers of Nordic and Baltic multinational security relationships. The government is a strong NATO Enhanced Opportunity Partner but has stopped short of seeking full membership in the alliance.

Looking at measurable components of capability, Sweden is a small power overall with significant capability to act in the information domain. Sweden's scores are similar, but less than, Australia in both average CINC score and the combined Belfer center average of Information Control and Norms. This makes Sweden another border case for considering whether it is a high or low capability state— it is a small state in the aggregate, but it has significant capabilities relevant to combatting disinformation. Specifically, it ranks in the smallest CINC quartile, and it is above average in the combined NCPI rankings. As for its Organization for Economic Cooperation and Development Trust rating, the Swedish government had an average trust rating among its people of 55%. That is the fifth highest average among all the states I sampled and just .0025 from scoring in the top quartile. These ratings make Sweden a high will, low capability state in my framework and the government's policies pursued from 2013-2020 do conform to the expectations.

Sweden employed several defensive efforts including alliances, multinational institutions, public education, and total defense concepts aimed at pushing back against Russian interference. The Swedish prime minister announced a new government agency with primary responsibility for building the population's psychological defense. The agency is called "psykolhgiskt forsvar." It had been disbanded in 2009, but by 2015, the

Swedish government brought[390] it back into operation. The government also in 2017 took several steps to push back against computational propaganda, a key driver in the speed and reach of propaganda in the digital age before the prime minister later publicly claimed that Russia was responsible for several operations ongoing in Sweden.[391] The Swedish government has also made a point of working with partners and allies. Although Sweden is not a NATO ally, it is an active partner nation. Sweden is a non-NATO member of NATO's Strategic Communications Center of Excellence.[392] It is a member of the European Union. It has tried to leverage its relationships with NATO and the European Union to track Russian strategic narratives and to elevate Russian malign influence as a security threat.[393] The government has supported European Union sanctions against Russia for its invasion of Ukraine. And, as mentioned in the Finland notes above, has partnered with Finland in issuing a joint statement condemning Russian influence operations in the Nordic states.[394] While partnering with other states, Sweden has also employed public education campaigns domestically. The Ministry of Defense conducted an awareness campaign about propaganda and the National Security Strategy names Russia's disinformation as a national security threat.[395] The Swedish government has also taken steps to protect democratic institutions.

Sweden has acted to protect its democratic institutions including the press, elections, and its civil service. The government proposed eliminating taxes on printed daily news

390. Jopling, 2018, Hanzelka and Pavlikova, 2021, and Wgnsson, 2020.
391. Hedman, 2018.
392. Hanzelka and Pavlikova, 2021.
393. Wagnsson, 2020.
394. Pynnöniemi, 2019.
395. Hanzelka and Pavlikova, 2021, and Wagnsson, 2020.

outlets.[396] This is designed to advantage local print media over the flood of disinformation on digital outlets which is comparatively much easier to use amplifying disinformation. Swedish officials also acted to protect elections, training local election workers on how to recognize and combat foreign attempts to attack elections.[397] Lastly, the government published a handbook for its domestic communicators to recognize and counter disinformation that might be used to target public employees.[398] Protecting these domestic democratic institutions demonstrates the government's will to resist Russian disinformation. Sweden has also worked to build resiliency in its population.

The Swedish policy approach from 2013-2020 has included many efforts aimed at cultivating resiliency within its people. The Swedish Civil Contingencies Agency (MSB) is specifically chartered "to have good capacity to identify and counter information influence activities and the spread of other deceptive information within its area of responsibility."[399] The Ministry of Defense's public education campaign already mentioned above includes a document "If Crisis or War Comes."[400] It is twenty pages long and details total defense strategies that Swedish people are expected to employ resisting any Ukraine-like hybrid invasion. The document had been delivered to households from World War II to the end of the Cold War, but the government resumed distributing it in 2018. This boosts resiliency in several ways: it highlights the seriousness of the resurgent Russian threat, elevating the threat in the mind of Swedes, and provides advice for what the population can do to resist disinformation. Further, the psychological

396. Haciyakupoglu, et al., 2018.
397. Jopling, 2018.
398. Hanzelka and Pavlikova, 2021.
399. Tofvesson, 2016.
400. Hanzelka and Pavlikova, 2021.

defense also mentioned above, reinforces a strategy of resiliency. Part of the Swedish approach to that defense includes identifying, analyzing, and responding to external influence.[401] Awareness of disinformation operations is a key way to blunt their effectiveness. By working to identify, analyze, and respond, the government is inoculating its population against the slow burn which results from ignoring disinformation. And the government takes further steps to build resiliency through multiple educational approaches. Education is not limited to civil servants and defense handbooks; media literacy is also taught in Swedish schools. Students are taught how to tell reliable from specious sources of information.[402] Finally, the government is working to integrate sectors to push back against disinformation. The government and Swedish national television have been experimenting in digital automatic fact checking capabilities that cuts across information silos and filter bubbles.[403] The Swedish government is doing everything that one would expect of a low capability democracy with high will to resist Russian disinformation.

In conclusion, it bears noting that Sweden is so attuned to disinformation that it had a uniquely shocking reaction to the Trump administration. Early in former President Trump's administration, he mentioned "You look at what's happening last night in Sweden" implying that there had been a violent attack in the country. There was no attack, and the comment made no sense except as amplifying right-wing disinformation, but instead of just shrugging and moving on to the next news cycle Sweden debated

401. Jopling, 2018.
402. Wagnsson, 2020, and Haciyakupoglu, et al 2018.
403. Hanzelka and Pavlikova, 2021.

concerns about United States influence activities.[404] Sweden's long history of partnership with NATO and the United States has been cultivated as means to defending itself from Soviet and Russian aggression. Their history and geography make them well attuned to Russian disinformation operations and it says a lot that a sitting United States President triggered their detection of influence operations.

High Will, High Capability (Canada, France, Germany, United Kingdom)

Coorelates of War CINC			NCPI Ranking (Information Control and Norms)			OECD Trust		
	Avg. 2013-16	Since 1991	State	Average		State	Average	
United States	0.13204	Q1	United States	1.0	Q1	Netherlands	61.31	Q1
Russia	0.03786	Max .15630	United Kingdom	7.0		Germany	58.83	Max 80.86
Germany	0.01688	Q2 .01998	Russia	7.5		Canada	58.02	
United Kingdom	0.01433		France	10.0	Q2 9.4	Finland	57.01	
France	0.01374		Australia	11.0		Sweden	55.48	Q2 55.73
Italy	0.01150		Sweden	11.0		Russia	51.57	
Canada	0.00861	Median .0104	Canada	12.5		Australia	45.66	
Spain	0.00764	(Q3 .02281)	Netherlands	14.0	Q3 12.8	United Kingdom	40.42	Q3 44.92
Australia	0.00674		Germany	15.5		France	36.22	
Poland	0.00549		Spain	17.5	Q4 16.0	United States	35.09	
Netherlands	0.00398	Q4 .00543	Lithuania	22.5		Lithuania	33.86	Q4 34.52
Sweden	0.00210	min .00039	Italy	24.0		Poland	33.11	Min 14.57
Finland	0.00151					Spain	29.10	
Lithuania	0.00041					Italy	25.19	

Table 21: Ratings for High Will, High Capability States

Legend:			Expected Action				
			Mix of direct (offensive) and indirect (defensive) efforts. Ex: punish attackers, educate population, build and	Canada	France	Germany	UK
Observed	High Will	High Capability	Protect democratic institutions, processes, and norms domestically and internationally	Canada	France	Germany	UK
Inconsistent			Leadership role integrating response to disinformation: domestically and internationally	Canada	France	Germany	UK
Not observed							

Table 22: Overall Findings for High Will, High Capability States

Canada

Canada is the least powerful of the high will high capability states. The lack of American leadership on promoting democratic norms and institutions abroad has likely made the Canadian Government shoulder even more responsibilities than it otherwise

404. Wagnsson, 2020.

would. It has strengthened its elections and laws at home and led the creation of new international organizations to coordinate disinformation responses internationally. Further, Canada is likely to come into more direct conflict with Russia as the two states compete in a warming Arctic.

In my sample of states, Canada is in the middle of the pack for its ratings in Correlates of War CINC rating and in the Belfer Center's NCPI rankings. Specifically, Canada ranks 6 of 13 with an average CINC score of .00861, just below the median score for the sample. And it ranks 7 of 13 among the states for the Belfer Center's rankings of Information Control and Norms. So, it could not be more squarely in the middle of the sample's power rankings. Since the states in my sample are mostly rich Western democracies, being in the middle of the sample indicates Canada is a highly capable state. In terms of Organization for Economic Cooperation and Development Trust, Canada placed higher among the sample. Its government's average score from 2012 to 2020 was 58% trust— third highest in the sample as rated according to its own people. According to my classification, Canada is therefore high will and high capability. The Canadian governments actions taken 2013-2020 regarding Russian disinformation mostly conform to expectations, but with some exceptions.

First, while Canada did employ a mix of offensive and defensive measures, it was mostly defensive and domestically focused instead of taking on Russia directly. Prime Minister Trudeau has named Russian disinformation as a serious threat and expelled Russian diplomats over interference in its democracy[405], but all other actions appear to be

405. India Blooms, 2020.

defensive. For example, Canada includes in its Criminal Code and Election Act offenses which could be used to make disinformation and false statements about candidates an offense if such acts are taken to influence an election.[406] So while the threat of disinformation from Russia is from beyond Canadian borders, the main tools its government has for punishing disinformation is focused on domestic actors. This is defensive since it responds to an attack but seems unlikely to preempt or deter Russian aggression. In fact, the main actions taken in Canada seem focused on the second expected course of action: protect democratic institutions.

Next, Canada significantly acted from 2013-2020 to protect democratic institutions, at home and abroad. This is in line with predictions for a high will high capability state. Canada particularly focused on protecting its elections. There, Elections Canada has responsibility for running federal elections. Elections Canada is an independent agency, but it integrates its efforts with other Canadian government capabilities to identify threats, tactics, and vulnerabilities. The Security Intelligence Service and Communications Security Establishment both work with Elections Canada to secure elections.[407] Elections have also been bolstered through legislation. The Elections Modernization Act requires enhanced transparency and reporting requirements of digital platforms including prohibition of foreign entities' purchase of ads during an election period. Online outlets must disclose purchasers of ads related to federal elections, keep the ads for two years in a registry, and maintain the information related to transactions for

406. Levush, 2019.
407. Levush, 2019.

five years beyond that.[408] Additionally, the government bolstered democratic norms domestically and in support of democracy globally. It adopted a digital charter with popular feedback that emphasizes democratic values, prioritizes election security, and implements strategies to inform candidates, organizations, and officials when they are known targets of an attack.[409] Internationally, Prime Minister Trudeau acted to bolster efforts at pushing back against disinformation and extremism. He announced in 2019 that Canada would join the Christchurch Call along with New Zealand and France following the livestreaming of a New Zealand mass shooting attack. Although the Christchurch Call is aimed at terrorist and extremist content, there is overlap with disinformation since many misnamed "lone wolf" attacks are brought into the physical world through international propaganda networks organized and inspired online.[410] Canada has promoted democratic norms and institutions. The government has taken a leadership role in coordinating responses to malign Russian influence.

Finally, the Canadian government took a leadership role integrating domestic and international responses to Russian disinformation. It created new organizations like the Security and Intelligence Threats to Elections (SITE) Task Force and lead the G7 Rapid Response Mechanism setup in 2018 as part of a joint response protecting democratic processes from increasing threat.[411] It pledged CAN$7 million in media literacy efforts ahead of its 2019 federal election, implemented the Critical Election Incident Public Protocol to inform the public of election integrity threats, and put Russian interference in

408. Levush, 2019.
409. Levush, 2019.
410. Belew, 2019.
411. Levush, 2019.

mainstream discussions during the 2019 election.[412] All of these actions led or helped lead response to Russian influence. Canada also responded with more than words; in 2020 it had 600 Soldiers in Latvia leading a multinational force on Russia's border bolstering NATO efforts to deter Russian aggression in the Baltics. The mission naturally became the target of Russian disinformation operations. Canada pushed back against false narratives and remained steadfast there in its mission.[413]

Canadian response to Russian disinformation from 2013-2020 largely conformed to expectations for a high will, high capability state. It likely filled some roles that the United States historically would have filled when led by a President not enamored with employing rather than combatting disinformation tactics. For example, the United States did not sign on to the Christchurch Call until after President Trump left office and at most times, the United States likely could have been expected to lead the G7 Rapid Response Mechanism. Canada continues to earn the trust of its population and has worked to protect its democracy from Russian attack. In coming decades, Canada will likely need to become even stronger in its efforts; already a target of influence operations, it will likely come under increasing challenge from Russia as the two states draw into more direct competition in a warming Arctic.[414]

France

Over the 2013-2020 period, France has been the clearest leader for promoting democratic institutions and multinational approaches to Russian disinformation. France

412. Tsurkan, 2020, and Levush, 2019.
413. Chase, 2020, and Brewster, 2020.
414. Sukhankin, 2019.

has acted to protect its own elections and its policies have been models for approaches adopted by both the European Union and major social media companies. Of the three European states in the high will high capability grouping, only France has both avoided catastrophic interference in its politics and been unequivocally critical of Russian malign influence.

The French government's actions are a clear demonstration of predictions for a high will high capability state. It is above average for both CINC and Belfer Center rankings. France's average CINC from 2013-2016 made it the fourth most powerful state among my sample of democracies, scoring very close to the United Kingdom for that period. The Belfer Center rankings for Information Control and Norms also put France high among democracies; only the United States and the United Kingdom ranked higher. France's Organization for Economic Cooperation and Development Trust score was not so high. On average, only 36% of French respondents expressed trust in their government from 2012-2020. While this score also ranks closely with the United States and United Kingdom, it is still below average for the sample. Considering the other elements of will, however, the French government has demonstrated high will through statements and actions counteracting Russian disinformation. The government has employed a mix of offense and defense, bolstered democratic institutions and norms, and it has led— domestically and internationally— pushing back against Russian malign influence.

France's national government has combined direct and indirect measures to fight Russian disinformation. Part of France's high Belfer ranking include its effectiveness fighting jihadist information operations during the early part of this dissertation's

considered period. France experienced several violent attacks inspired and facilitated through extremist organizations adept at online recruitment, organization, and amplification.[415] The government gained experience combatting the spread of propaganda and used those to confront Russian efforts. Direct examples include clear statements and actions from the highest levels. As a candidate, Emanuel Macron warned about Russian interference.[416] His team hired experts to plant decoys, feed bad information to Russian hackers, and prepare a communications strategy to combat leaked information.[417] Further, France's National Commission for the Control of the Electoral Campaign for the Presidential Election and the National Cybersecurity Agency had responsibility for protecting the election. Within hours of a data leak during the 2017 election, French law enforcement began a criminal investigation.[418] Indirectly, the government has called on its public schools to teach students about critically assessing trustworthiness of online sources.[419] And after winning election as President, Macron banned RT and Sputnik from his media pool. He said they are not journalists, but agents of influence.[420] The French Government followed suit labeling them "Pro-Kremlin outlets."[421] This combination of direct and indirect actions have the combined effect of limiting in France key nodes Russia employs elsewhere while building French sensitivity to the threat. France has also designed laws and policies that protect democratic institutions.

415. Šramková, 2018.
416. Hanzelka and Pavlikova, 2021
417. Jopling, 2018, and Davis, 2018.
418. Levush, 2019.
419. Levush, 2019.
420. Jopling, 2018.
421. Hanzelka and Pavlikova, 2021

France was a leader 2013-2020 protecting democratic processes and norms. Domestically, it has empowered its Superior Council of the Audiovisual (CSA) to remove online content, accounts, and websites to prevent disinformation from spreading during an election. Also, French candidates and parties can petition a judge on removing disinformation within 48 hours.[422] And, in 2017 after the data breach, the French government warned not only its citizens that there had been a breach, but also warned platforms operating in the country that spreading the hacked and leaked information could be grounds for criminal prosecution.[423] The government was active in France particularly around the election of 2017. In 2018, it strengthened its laws to limit disinformation. France requires platforms with greater than five million users to disclose authors and amounts paid for sponsoring content.[424] It also requires platforms that employ algorithms to disclose detailed statistics about how the site works and how content is shared including "how many times pieces of content are accessed directly; accessed through platform recommendation, sorting, reference algorithms; accessed through platform's internal search."[425] France's domestic efforts have also made it a leader protecting democracy internationally. In addition to hosting the Christchurch conference after the attack in New Zealand, President Macron has appealed to the citizens of Europe advocating the creation of a new European Union agency for democracy protection and fighting hate speech.[426] It would not be the first time French thought had led the Continent. Some European Union-wide laws are already based on French law.

422. Jopling, 2018, Hanzelka and Pavlikova, 2021, Davis, 2018, and Durach, 2020.
423. Levush, 2019.
424. Šramková, 2018.
425. Levush, 2019.
426. Šramková, 2018.

Further, large media organizations like Facebook and Twitter have themselves chosen to apply French standards to their operations throughout the European Union.[427]

France has been active at home and abroad in developing policies to combat disinformation. Its mix of direct and indirect responses, protection of democratic institutions, and leadership internationally all conform to expectations for a high will high capability state fighting Russian disinformation.

Germany

The German Government's responses in this period were least consistent with expectations of a high will high capability state. Rather than being a strong leader for democratic norms and institutions, Germany sometimes took both sides of major issues involving Russian attacks on democracy in Europe and globally. Germany's postwar pacifism, its history as ground zero for Cold War disinformation and espionage, and Russian sympathies in its population likely account for its pragmatism.

Germany is the second most powerful democracy in my sample, and one with high trust in government among its people. However, its governmental capabilities put against the disinformation threat and its lack of overt international leadership from 2013-2020 did not fully conform to expectations for a high will high capability state. Considering Germany's historical and geographic context, the lack of enthusiasm for direct confrontation with Russia on this issue makes more sense.

Germany is overall very powerful. It is the second highest Correlates of War CINC score among democracies in my sample and is the most powerful democracy in Europe.

427. Levush, 2019.

Alone, it scores nearly half of Russia's CINC average from 2013-2016. When combined with either France or the United Kingdom, either pairing exceeds Russia's score. Herein lies Russia's strategic imperative for weakening the European Union and NATO from within— Russia is stronger than any European state on a one-to-one comparison but competes from a position of asymmetric weakness when dealing with a united bloc. Germany, however, has not been as publicly active as France pushing back against attacks on democratic institutions or in leading development of international responses to disinformation. The result shows in the Belfer center's rankings where Germany is only just above the lowest quartile for cyber capabilities useful combatting disinformation. Still, Germany enjoyed high levels of trust in government as expressed by its people 2012-2020. An average of 59% of those asked said they trusted the German government during that period. Only the Netherlands scored higher. Germany's history and geography help explain how Germany has chosen to respond firmly, but quietly to the Russian threat and why it maintains a level of trust among Germans.

First, the actions that Germany took were mostly defensive. The government recognizes the threat. Its Bundesamt für Verfassungsschutz (BfV or Office for Protection of the Constitution) recognizes and considers RT DE an arm of Russian influence operations in Germany.[428] German officials have named Russia for hacking parliament and for the "Our Lisa" protests Russia fomented across Germany during the Syrian refugee crisis.[429] Because of its history with totalitarianism and as a hotbed of Cold War espionage and disinformation, German law prohibits broadcasting by state agencies.

428. Yerepouni Daily News, 2021.
429. Davis, 2018, and Steizenmuller, 2017.

Recent German law also requires platforms to remove posts that "seek to disseminate propaganda material or use symbols of unconstitutional organizations; encourage the commission of a serious violent offense, endanger the state; and advocate the commission of treasonous forgery, public incitement to crime, and a incitement to hatred."[430] Under the law, the 2017 Network Enforcement Law or NetzDG, platforms can be fined up to €50 million[431] and the government fined Facebook €2 million[432] soon after passing the law. In addition to defensive laws, the German Government has pursued a range of public education campaigns, particularly aimed at its youth, parents, and civics. Examples include "Ein Netz fur Kinder" (an internet for kids), "Shau Hin!" (look at!), "Demokratielobore" (Democracy laboratories). These sites provide extensive guides, reviews, information, and practical advice for protecting children and citizens from online harms including disinformation and radicalization. They also promote understanding of the duties demanded by democratic participation for both kids and older citizens.[433] These efforts are all defensive, however, not aimed at Russian propagandists but at inoculating Germans. The defensive approach extends to institutions, particularly elections.

Second, the government has acted to bolster democratic norms and institutions but not in the way predicted by a state of its power and elevated trust. Germany's efforts to protect democracy have been mostly aimed domestically, not so much in rallying international efforts. At the same time that Russia was interfering with Brexit and the

430. Levush, 2019.
431. Jopling, 2018.
432. Levush, 2019.
433. Levush, 2019.

2016 United States Presidential election, Russia also hacked the German Parliament.[434] Both Chancellor Merkel, herself having grown up with personal experience of Soviet influence operations and the East German Stasi, and also the head of Germany's domestic intelligence agency warned Germans— and Russians— about using the stolen data during Germany's 2017 elections.[435] Germany further protects its elections by using paper ballots[436] and, ahead of the 2017 election, German political parties agreed not to employ leaked information or bots on social media.[437] These steps appear to have been sufficient in preventing Russia's decision to use the stolen data in Germany's election after having just successfully attacking the United Kingdom's Brexit referendum and the 2016 United States election.[438] Although my focus intentionally avoids state actions that may have been taken beyond those publicly reported, besides warnings, Germany did not directly confront or punish Russia for disinformation operations in Germany. That is clearly a choice since Germany has taken direct action against Russia for other actions and at other times. Specifically, Germany called for increased sanctions against Russia after its 2020 hybrid attack against Alexi Navalny. The German Government almost certainly saved Navalny's life by demanding his release from Russia and providing medical treatment.[439] The German Government does coordinate up— at the European Union level to prevent hate speech and disinformation, and down—to support regional communications countermeasures both online and offline within Germany.[440] Its defense

434. Jopling, 2018, and Polyakova and Boyer, 2018.
435. Polyakova and Boyer, 2018, and Hanzelka and Pavlikova, 2021.
436. Steizenmuller, 2017.
437. Hanzelka and Pavlikova, 2021.
438. Polyakova and Boyer, 2018.
439. Baczynska, 2021.
440. Levush, 2019.

of democratic institutions from 2013-2020 was mostly domestic, however, not as a leader of international responses. This makes sense given its history and geography.

As mentioned, Germany has long experience with Russian and Soviet disinformation. Following World War II, Germany remained divided as recently as 1989. It was the epicenter and a literal battle line for the Cold War between the United States and the Soviet Union. Long lasting impacts of Russian political warfare and disinformation were felt by Germans in Germany. Additionally, because many of its people lived in the Soviet sphere for so long, because the East remains economically unequal to its West, and because there exists native Euroscepticism, there are segments of the population which, if they do not identify as Russians, certainly are more open to "understanding" Russia and Vladimir Putin.[441] The German Government, then, understandably is more muted in how and when it responds to Russia, especially compared to other powerful European democracies like France and the United Kingdom. As such, it did not act exactly as expected of a high will high capability state. It was more restrained internationally than predicted.

United Kingdom

The United Kingdom suffered the biggest Russian disinformation success during this period with the sole exception of the 2016 United States Presidential election. Brexit, combined with the assassination of multiple former Soviet spies on British soil, caused the government to take an active role developing domestic policy to bolster elections, national security, and public awareness of Russian disinformation. Additionally, the

441. Wood, 2020.

United Kingdom developed new governmental agencies with the mission to coordinate responses to, and to generally deter, Russian disinformation. With the major exception of Brexit, the United Kingdom has been a leader in aggressively pushing back against Russian influence.

Besides the United States, the United Kingdom has been the most frequent target of Russian influence operations. It has also been the site for two key grey zone attacks including Brexit referendum interference and the attempted murder of Sergei Skripal by Russian agents in Salisbury. The United Kingdom has been aggressively targeted because it is a leading democracy. Its power and prestige make it a high payoff target. According to the Correlates of War project, the United Kingdom's average CINC from 2013-2016 was in the top three among the democracies in my sample. And, according to the Belfer Center, the United Kingdom is only behind the United States in demonstrated abilities regarding information control and norms. These factors combine to make the United Kingdom one of the most powerful states in my sample. The United Kingdom is a middling democracy, however when it comes to its people's expressed trust in their government. Between 2012 and 2020, the United Kingdom government's Organization for Economic Cooperation and Development trust rating was just below average at 40% confidence among its population. Assessing the government's reaction, it seems that the United Kingdom behaved in a manner like Germany. That is, it is certainly high capability and demonstrated high will, but it did not totally conform to what the expectations for such a state dealing with Russian aggression.

First, the United Kingdom did employ a mix of direct and indirect responses to Russian attacks. At a basic level, the United Kingdom government and parliament undertook a series of investigations to define terms and determine practical steps for defending against Russian disinformation. The Digital, Culture, Media, and Sport Committee (DCMS), for example, recommended doing away with the term "fake news" in favor of using clearly defined terms like misinformation and disinformation.[442] The government published a white paper called "Online Harms" which made recommendations on new accountability for online platforms including a legal "duty of care" standard for content and a requirement to remove harmful content.[443] Other defensive approaches included expanding the National Security Communications Team (NCST) and establishing a Rapid Reaction Unit (RRU). The NCST has responsibility to deter state actors and others as part of an overall Fusion Doctrine that elevates strategic communications to the same level as military and financial elements of national response options aimed at achieving national security goals. The RRU is a Cabinet level agency that bridges defense and offense. Generally, the RRU takes two approaches to disinformation; it has a playbook for identifying and responding to threats around predictable events like elections and it has an established procedure to guide reactions to unanticipated attacks. Both seek to increase the availability of reliable government information that remain visible to the public in an attack. During one disinformation operation which sought to mislead people about a Syrian airstrike, for example, the RRU was able to move official United Kingdom information to the top of search algorithms

442. Levush, 2019 and Davis, 2018.
443. Levush, 2019.

which otherwise were burying official information into the 200th-most popular recommendation behind many specious sources.[444] The government has also launched many education campaigns for its population and government. The NCST uses a SHARE construct in a "Don't Feed the Beast" campaign. SHARE is a checklist that reminds users to critically consider Source, Headline, Analyze, Retouched, Error attributes of online sources. The RRU follows a FACT construct to guide its focus: Find, Assess, Create, and Target. SHARE is useful for individuals, RRU is useful for communications strategists.[445] Early in the 2013-2020 period, the United Kingdom was focused mainly defensively. This makes sense considering it was during this time that the government was sorting through Russia's role in the Brexit referendum. Later in the period, the United Kingdom began acting more rapidly and directly to confront Russian aggression. Within weeks of the attempted murder of Sergei Skripal, the United Kingdom government had established the RRU to take back a fact based narrative and British spies and police gathered enough evidence to rally expulsion of Russian spies internationally. This response also demonstrated that the government learned from Russia's 2006 poisoning murder in the United Kingdom of Alexander Litvinenko.[446] The United Kingdom became more sensitive to the disinformation threat over this period and began acting with greater speed confronting Russian disinformation. Its focus on democratic norms also began to shift during the period.

444. Levush, 2019.
445. Levush, 2019.
446. Grey Zone, Episode 1.

Second, the United Kingdom defended norms domestically, but not until after the Brexit referendum attack. Prime Minister Johnson, who would not be Prime Minister but for his promises to deliver on the slim majority of "leave" votes in the Brexit referendum publicly warned his pubic about Russian interference in British elections.[447] Also, the aforementioned "Online Harms" white paper recommended steps for protecting elections. Freedom of expression is a qualified right in Britain, meaning it can be curtailed when doing so is in furtherance of a legitimate democratic goal. Protecting elections is one such aim.[448] Like the United States, many election norms were informal. The United Kingdom's Electoral Commission made recommendations to codify many of those norms including increased reporting requirements for online ads targeted at users through demographic information, banning foreign money in British elections, and generally maintaining a "follow the money" approach to creation of election rules. The commission also recommended that new rules were vital since current British law is "not fit for purpose." For example, political ads are prohibited in broadcast media and there are restrictions on commercial ads, but there is no regulation of digital political advertisements.[449] The United Kingdom approach for this period focused more on the domestic fallout from the Brexit referendum and was not as focused on international democracy as my theory would predict.

Finally, the domestic focus extended to coordination of responses. Another government document during this period outlined the argument that the government

447. Hanzelka and Pavlikova, 2021.
448. Levush, 2019.
449. Levush, 2019.

needed to coordinate policy to protect domestic journalism. The Cairncross Review concluded that there is a supply side market failure in public interest media production which threatens the health of British democratic debate and collective decision making.[450] The United Kingdom security and intelligence services also recommend that the government needs to address disinformation as a national security threat. The government considers malign influence operations as "fourth generation espionage" and highlights the need to coordinate society-wide efforts protecting against not only physical threats but also "cognitive attack and subversion."[451] The major recommendations for United Kingdom Government action against disinformation include regulating online platforms, rebalancing relationship between publishers and platforms, creating a new institute for the future of public-interest news, tax law incentivizing payment for online news, and media literacy strategy.[452] While the United Kingdom does provide senior level employees at the NATO Strategic Communications Center of Excellence,[453] and while it has in recent years started taking the lead internationally in some instances punishing Russian disinformation, from 2013-2020 the United Kingdom was more domestically oriented than my theory would predict for a leading democratic state.

450. Levush, 2019.
451. Levush, 2019.
452. Levush, 2019.
453. Hanzelka and Pavlikova, 2021.

BIBLIOGRAPHY

Acemoglu, Daron, and James A. Robinson. *Economic Origins of Dictatorship and Democracy*. Cambridge Univ. Press, 2006.

Ajir, Media, and Bethany Vailliant. "Russian Information Warfare: Implications for Deterrence Theory." *Strategic Studies Quarterly*, vol. 12, no. 3, 2018, pp. 70–89.

Allcott, Hunt, et al. "Trends in the Diffusion of Misinformation on Social Media." *Research & Politics*, vol. 6, no. 2, Apr. 2019.

Applebaum, Anne. "The Bad Guys Are Winning." *The Atlantic*, 15 Nov. 2021, https://www.theatlantic.com/magazine/archive/2021/12/the-autocrats-are-winning/620526/.

---. "The Science of Making Americans Hurt Their Own Country." *The Atlantic*, Mar. 2021.

---. *Twilight of Democracy: The Seductive Lure of Authoritarianism*. First edition, Doubleday, 2020.

Applebaum, Anne, and Peter Pomerantsev. "How to Put Out Democracy's Dumpster Fire." *The Atlantic*, Mar. 2021, https://www.theatlantic.com/magazine/archive/2021/04/the-internet-doesnt-have-to-be-awful/618079/.

Apuzzo, Matt, and Adam Satariano. "Russia Is Targeting Europe's Elections. So Are Far-Right Copycats." *The New York Times*, 12 May 2019. https://www.nytimes.com/2019/05/12/world/europe/russian-propaganda-influence-campaign-european-elections-far-right.html.

Baczynska, Gabriela. "Germany Is Main Target of Russian Disinformation, EU Says." *Reuters*, 9 Mar. 2021, https://www.reuters.com/article/us-eu-russia-germany-idUSKBN2B11CX.

Baumann, Mario. "'Propaganda Fights' and 'Disinformation Campaigns': The Discourse on Information Warfare in Russia-West Relations." *Contemporary Politics*, vol. 26, no. 3, May 2020, pp. 288–307.

Bechis, Francesco. "Infodemic in Italy." *Center for European Policy Analysis*. 27 May 2020, https://cepa.org/infodemic-in-italy/.

Beckley, Michael. "The Power of Nations: Measuring What Matters." *International Security*, vol. 43, no. 2, Nov. 2018, pp. 7–44.

---. *Unrivaled: Why America Will Remain the World's Sole Superpower*. Cornell University Press, 2018.

Belew, Kathleen. *Bring the War Home: The White Power Movement and Paramilitary America*. Harvard University Press, 2019.

Benkler, Yochai, Casey Tilton, et al. "Mail-In Voter Fraud: Anatomy of a Disinformation Campaign." SSRN Scholarly Paper, ID 3703701, *Social Science Research Network*, 2 Oct. 2020.

Benkler, Yochai, Rob Faris, et al. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press, 2018.

Bennett, W. Lance, and Steven Livingston. "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions." *European Journal of Communication*, vol. 33, no. 2, Apr. 2018, pp. 122–39.

Beskow, David M., and Kathleen M. Carley. "Characterization and Comparison of Russian and Chinese Disinformation Campaigns." *Disinformation, Misinformation, and Fake News in Social Media*, edited by Kai Shu et al., Springer International Publishing, 2020, pp. 63–81.

Bjola, Corneliu, and Krysianna Papadakis. "Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience." *Cambridge Review of International Affairs*, vol. 33, no. 5, Sept. 2020, pp. 638–66.

Bodine-Baron, Elizabeth, et al. "Countering Russian Social Media Influence." *RAND Corporation*, 2018.

Bond, Shannon, and Bobby Allyn. "The Facebook Whistleblower's Documents Show How "Stop the Steal" Evaded Monitors." *NPR*. 22 Oct. 2021, https://www.npr.org/2021/10/22/1048543513/facebook-groups-jan-6-insurrection.

Booth, William, and Michael Birnbaum. "British and Spanish Leaders Say Russian Trolls Meddled in Their Elections." *Washington Post*, 14 Nov. 2017. www.washingtonpost.com, https://www.washingtonpost.com/world/europe/britain-and-spanish-leaders-say-russian-trolls-meddled-in-their-elections/2017/11/14/51ffb64a-c950-11e7-b506-8a10ed11ecf5_story.html.

Borovoy, Konstantin. *Russia Against USA: Russia's Disinformation Campaign against USA and Its Citizens*. Independently Published, 2020.

Bradshaw, Samantha, and Philip N. Howard. "The Global Organization of Social Media Disinformation Campaigns." *Journal of International Affairs*, vol. 71, no. 1.5, 2018, pp. 23–32.

Brewster, Murray. “Canadian-Led NATO Battlegroup in Latvia Targeted by Pandemic Disinformation Campaign.” *The Canadian Broadcasting Corporation*, 24 May 2020, https://www.cbc.ca/news/politics/nato-latvia-battle-group-pandemic-covid-coronavirus-disinformation-russia-1.5581248.

Bunyan, Rachael, and Walter Finch. “Putin’s Warning for the West: Vladimir Vows “consequences” for Those Who Interfere in Ukraine.” *Daily Mail Online*. 12 Apr. 2022, https://www.dailymail.co.uk/news/article-10710541/Russia-moves-military-equipment-Finnish-border-warning-Finland-not-join-NATO.html.

Butt, Shelby, and Daniel Byman. “Right-Wing Extremism: The Russian Connection.” *Survival*, vol. 62, no. 2, Mar. 2020, pp. 137–52.

“Canada PM Trudeau Cites ‘disinformation Campaign’ on Russian Interference.” *India Blooms*, 5 Apr. 2018.

“Canadian Professor’s Website Helps Russia Spread Disinformation, Says United States State Department.” *The Canadian Broadcasting Corporation*, 2020.

Charon, Paul, and Jean-Baptiste Jeangène Vilmer. *Chinese Influence Operations: A Machiavellian Moment*. Institute for Strategic Research (IRSEM), Paris, Ministry for the Armed Forces, Oct. 2021, https://www.irsem.fr/report.html.

Chase, Steven. “Lithuania Requests Canada’s Help in Combatting Russian Disinformation.” *Globe & Mail*, 29 Feb. 2020.

Čižik, Tomáš. *Information Warfare - New Security Challenge for Europe.* 2017.

Cristiani, Dario. “The Paradox of Russia’s Disinformation Activities in Italy.” *Eurasia Daily Monitor*, vol. 17, no. 85, June 2020, https://jamestown.org/program/the-paradox-of-russias-disinformation-activities-in-italy/.

“Democracy Reports.” *V-Dem*. http://v-dem.net/democracy_reports.html. Accessed 23 Feb. 2022.

Dew, Andreaj. “Fighting for Influence in Open Societies: The Role of Resilience and Transparency.” *The Fletcher Forum of World Affairs*, 2019, p. 17.

DiResta, Renee, et al. “The Tactics & Tropes of the Internet Research Agency.” *United States Senate Documents*, Oct. 2019, https://digitalcommons.unl.edu/senatedocs/2.

---. “Free Speech Is Not the Same As Free Reach.” *Wired*, Aug. 2018, https://www.wired.com/story/free-speech-is-not-the-same-as-free-reach/.

Douglas, Christopher. “Religion and Fake News: Faith-Based Alternative Information Ecosystems in the United States and Europe.” *The Review of Faith & International*

Affairs, vol. 16, no. 1, Jan. 2018, pp. 61–73.

Durach, Flavia, et al. "Tackling Disinformation: EU Regulation of the Digital Space." *Romanian Journal of European Affairs*, vol. 20, no. 1, Jun. 2020.

"Democracy Index 2020: In Sickness and in Health?" *Economist Intelligence Unit*, https://www.eiu.com/n/campaigns/democracy-index-2020/. Accessed 14 June 2021.

Dwoskin, Elizabeth, and Eugene Scott. "Obama Says Tech Companies Have Made Democracy More Vulnerable." *Washington Post*, 21 Apr. 2022. https://www.washingtonpost.com/technology/2022/04/21/obama-disinformation-stanford/.

Falandys, K., et al. "The Analysis of the Possibility of Carrying out Diversion and Disinformation on the Territory of the Republic of Poland in Connection with the War in Eastern Ukraine." *Zeszyty Naukowe*, vol. 3, 2016.

Flanagan, Stephen, et al. "Deterring Russian Aggression in the Baltic States Through Resilience and Resistance." *RAND Corporation*, 2019.

Freedman, Lawrence. *Strategy: A History*. Oxford University Press, 2013.

Frum, David. "The Enduring Lessons of the 'Axis of Evil' Speech." *The Atlantic*, 29 Jan. 2022, https://www.theatlantic.com/ideas/archive/2022/01/axis-of-evil-speech-frum-bush/621397/.

Galeotti, Mark. "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?" *Small Wars & Insurgencies*, vol. 27, no. 2, Mar. 2016, pp. 282–301.

Gamberini, Sarah Jacobs. "Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns." *Joint Force Quarterly*, 2020.

Gera, Vanessa. "Poland Targeted by Disinformation Attack, Suspects Russia." *AP News*, 25 Apr. 2020, https://apnews.com/article/6deaf2d6b2e5cdadac2722bb72e25934.

Gerdziunas, Benas. "Lithuania Hits Back at Russian Disinformation." *DW.COM*, 27 Sept. 2018, https://www.dw.com/en/lithuania-hits-back-at-russian-disinformation/a-45644080.

Gessen, Masha. *Surviving Autocracy*. Riverhead Books, 2021.

Giannetti, William. "A Duty to Warn: How to Help America Fight Back Against Russian Disinformation." *Air and Space Power Journal*, vol. 31, no. 3, Sept. 2017, pp. 95–105.

Giles, Keir. "Russian Information Warfare." *The World Information War*, edited by

Timothy Clack and Robert Johnson, 1st ed., Routledge, 2021, pp. 139–61.

Giusti, Serena, and Elisa Piras, editors. *Democracy and Fake News: Information Manipulation and Post-Truth Politics*. Routledge, 2020.

"Global Trends 2040: A More Contested World." *The National Intelligence Council*, Mar. 2021, https://www.dni.gov/index.php/gt2040-home.

Golovchenko, Yevgeniy, et al. "State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation." *International Affairs*, vol. 94, no. 5, Sept. 2018, pp. 975–94.

Greig, J. Michael, and Andrew J. Enterline. "National Material Capabilities (NMC) Data Documentation Version 6.0." June 28, 2021.

Gregor, Miloš, and Petra Mlejnková, editors. *Challenging Online Propaganda and Disinformation in the 21st Century.* Springer International Publishing, 2021.

Haciyakupoglu, Gulizar, et al. Haciyakupoglu, Gulizar, et al. *COUNTERING FAKE NEWS: A SURVEY OF RECENT GLOBAL INITIATIVES*, S. Rajaratnam School of International Studies, 2018.

Hall, Holly Kathleen. "The New Voice of America: Countering Foreign Propaganda and Disinformation Act." *First Amendment Studies*, vol. 51, no. 2, July 2017, pp. 49–61..

Hanzelka, Jan, and Miroslava Pavlikova. "Chapter 7: Institutional Responses of European Countries." *Challenging Online Propaganda and Disinformation in the 21st Century*, Springer International Publishing, 2021.

Haynes, Deborah, and Chris Scott. "Into The Grey Zone." *Sky News Podcasts*. 2021. https://news.sky.com/story/into-the-grey-zone-podcast-episode-one-the-gathering-storm-12184704.

Haynes, William. "Balancing Neutrality Between Russia and NATO: The Case of Finland." *Georgetown Security Studies Review*, 29 Jan. 2017, https://georgetownsecuritystudiesreview.org/2017/01/28/balancing-neutrality-between-russia-and-nato-the-case-of-finland/.

Higgins, Andrew. "Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote." *The New York Times*, 16 Feb. 2017. https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html.

Hochschild, Arlie Russell. *Strangers in Their Own Land: Anger and Mourning on the American Right*. 2018.

Homans, Charles. “Trucker Protest Moved by More Than Opposition to Covid Mandates.” *The New York Times*, 19 Mar. 2022. https://www.nytimes.com/2022/03/19/us/politics/trucker-convoy-protest.html.

Homer-Dixon, Thomas. “The American Polity Is Cracked, and Might Collapse. Canada Must Prepare.” *Cascade Institute*, 2 Jan. 2022, https://cascadeinstitute.org/the-american-polity-is-cracked-and-might-collapse-canada-must-prepare/.

Horesh, Theo. *The Fascism This Time: And the Global Future of Democracy*. 2020.

Howard, Brad. “Russia’s Invasion of Ukraine Could Spark a NATO Defense Spending Spree.” *CNBC*, 1 Apr. 2022, https://www.cnbc.com/2022/04/01/why-russias-invasion-of-ukraine-could-spark-a-nato-spending-spree.html.

“How Women Are Singled out for Vile Abuse for Political Ends.” *The Economist*, Nov. 2019. https://www.economist.com/europe/2019/11/07/how-women-are-singled-out-for-vile-abuse-for-political-ends.

Humprecht, Edda, et al. “Resilience to Online Disinformation: A Framework for Cross-National Comparative Research.” *The International Journal of Press/Politics*, vol. 25, no. 3, July 2020, pp. 493–516.

Iancu, Niculae, et al. *Countering Hybrid Threats: Lessons Learned from Ukraine*. IOS Press, 2016.

Irwin, Galen A., and Joop J. M. van Holsteyn. “Keeping Our Feet Dry: Impediments to Foreign Interference in Elections in the Netherlands.” *Election Law Journal: Rules, Politics, and Policy*, vol. 20, no. 1, Mar. 2021, pp. 54–69.

Jackson, Michael, and Paul Lieber. “Countering Disinformation: Are We Our Own Worst Enemy?” *The Cyber Defense Review*, vol. 5, no. 2, 2020, pp. 45–56.

Jamieson, Kathleen Hall. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President What We Don’t, Can’t, and Do Know*. Oxford University Press paperback, Oxford University Press, 2020.

Janda, Jakub. “How to Boost the Western Response to Russian Hostile Influence Operations.” *European View*, vol. 17, no. 2, Oct. 2018, pp. 181–88.

Jankowicz, Nina. *How to Lose the Information War: Russia, Fake News, and the Future of Conflict*. I.B. Tauris, 2020.

---. “The Disinformation Vaccination.” *The Wilson Quarterly*, vol. 42, no. 1, Jan. 2018.

---. “The Growing Threat of Domestic Disinformation in Poland.” *The Rule of Law Post*, 20 Aug. 2020, https://www.law.upenn.edu/live/news/10368-the-growing-threat-of-

domestic-disinformation-in/news/cerl-news.

Jonsson, Oscar, and Robert Seely. “Russian Full-Spectrum Conflict: An Appraisal After Ukraine.” *The Journal of Slavic Military Studies*, vol. 28, no. 1, Jan. 2015, pp. 1–22.

Kalan, Dariusz. “Poland’s State of the Media.” *Foreign Policy*, 25 Nov. 2019, https://foreignpolicy.com/2019/11/25/poland-public-television-law-and-justice-pis-mouthpiece/.

Kao, Craig Silverman, Jeff. “Infamous Russian Troll Farm Appears to Be Source of Anti-Ukraine Propaganda.” *ProPublica*, https://www.propublica.org/article/infamous-russian-troll-farm-appears-to-be-source-of-anti-ukraine-propaganda?token=RSKs73yklfmmU991twpwzhmNVtYB2kvy. Accessed 4 Apr. 2022.

Kanet, Roger E., editor. *Routledge Handbook of Russian Security*. Routledge, Taylor & Francis Group, 2021.

Kasparov, G. K., and Mig Greengard. *Winter Is Coming: Why Vladimir Putin and the Enemies of the Free World Must Be Stopped*. First edition, PublicAffairs, 2015.

Kaye, David. *Speech Police: The Global Struggle to Govern the Internet*. Columbia Global Reports, 2019.

Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy.* 1984.

Kivinen, Markku, and Katri Pynnöniemi, editors. *Beyond the Garden Ring: Dimensions of Russian Regionalism*. Kikimora Publications : Aleksanteri Institute, 2002.

Kleinfeld, Rachel. “The Rise of Political Violence in the United States.” *Journal of Democracy*, vol. 32, no. 4, 2021, pp. 160–76.

Kofman, Michael, et al. “Russian Military Strategy: Core Tenets and Operational Concepts.” *Center for Naval Analyses*, Aug. 2021.

Kosc, Wojciech. “Polish Reporters Worry about Newspapers Turning into ‘Hard-Line Propaganda’ Outlets.” *POLITICO*, 14 Dec. 2020, https://www.politico.eu/article/poland-media-democracy-kaczynski-censorship-polish-reporters-worry-about-newspapers-turning-into-hardline-propaganda-outlets/.

Kragh, Martin, and Sebastian Åsberg. “Russia’s Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case.” *Journal of Strategic Studies*, vol. 40, no. 6, Sept. 2017, pp. 773–816.

Kuklinski, James H., Paul J. Quirk, Jennifer Jerit, David Schwieder, and Robert F. Rich.

"Misinformation and the Currency of Democratic Citizenship." *The Journal of Politics*, vol. 62, no. 3, 2000, pp. 790–816.

Kuehn, Kathleen M., and Leon A. Salter. "Assessing Digital Threats to Democracy, and Workable Solutions: A Review of the Recent Literature." *International Journal of Communication (Online)*, Apr. 2020, pp. 2589–611.

Langfitt, Frank. "Finland Moves Closer to Seeking NATO Membership as the War in Ukraine Unites Europe." *NPR*, 13 Apr. 2022. https://www.npr.org/2022/04/13/1092686626/finland-moves-closer-to-seeking-nato-membership-as-the-war-in-ukraine-unites-eur.

"Languages of Finland - Institute for the Languages of Finland." *Kotimaisten Kielten Keskus*, https://www.kotus.fi/en/on_language/languages_of_finland. Accessed 7 Mar. 2022.

Lanoszka, Alexander. "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe." *International Affairs*, vol. 92, no. 1, Jan. 2016, pp. 175–95.

Larsson, Anders Olof. "Right-Wingers on the Rise Online: Insights from the 2018 Swedish Elections." *New Media & Society*, vol. 22, no. 12, Dec. 2020, pp. 2108–27.

Levitsky, Steven, and Daniel Ziblatt. *How Democracies Die*. First edition, Crown, 2018.

Levush, Ruth. "Government Responses to Disinformation on Social Media Platforms: Argentina, Australia, Canada, China, Denmark, Egypt, European Union, France, Germany, India, Israel, Mexico, Russian Federation, Sweden, United Arab Emirates, United Kingdom." *Law Library of Congress, Global Legal Research Directorate*, Sep. 2019.

Lewis, Michael. *The Fifth Risk*. First edition, W.W. Norton & Company, 2018.

Lieberthal, Kenneth G. "The American Pivot to Asia." *Brookings*, Dec. 21, 2011, https://www.brookings.edu/articles/the-american-pivot-to-asia/.

"Lithuanians Are Using Software to Fight Back against Fake News." *The Economist*, Oct. 2019. https://www.economist.com/science-and-technology/2019/10/24/lithuanians-are-using-software-to-fight-back-against-fake-news.

Lomas, Dan. "Ukraine and Intelligence Prebuttal: A Quick Post-Mortem." *RUSI*. 24 Feb. 2022, https://rusi.org/explore-our-research/publications/commentary/ukraine-and-intelligence-prebuttal-quick-post-mortem.

Lucas, Edward, et al. "Close to the Wind: What Russia Wants." *Center for European*

Policy Analysis, 9 Sept. 2021, https://cepa.org/baltic-sea-security-what-russia-wants/.

Lukito, Josephine. "Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three United States Social Media Platforms, 2015 to 2017." *Political Communication*, vol. 37, no. 2, Mar. 2020, pp. 238–55.

Martin, Diego A., Jacob N. Shapiro, and Julia G. Ilhardt. *Trends in Online Influence Efforts. Version 2.0.* Aug. 5, 2020.

Mason, Lilliana. *Uncivil Agreement: How Politics Became Our Identity.* The University of Chicago Press, 2018.

Matishak, Martin. "Intelligence Community Creating Hub to Gird against Foreign Influence." *POLITICO*, https://www.politico.com/news/2021/04/26/intelligence-community-hub-foreign-influence-484604. Accessed 27 Apr. 2021.

Mattis, Jim. Summary of the 2018 National Defense Strategy.

Maxwell, Joseph Alex. *Qualitative Research Design: An Interactive Approach*. 3rd ed, SAGE Publications, 2013.

McGeehan, Timothy P. "Countering Russian Disinformation." *Parameters*, vol. 48, no. 1, Mar. 2018, pp. 49–58.

McKay, Spencer, and Chris Tenove. "Disinformation as a Threat to Deliberative Democracy." *Political Research Quarterly*, vol. 74, no. 3, Sept. 2021, pp. 703–17.

McKeen, Alex. "Why Canada Appears to Be One of the Top Spreaders of Russian Disinformation Online." *The Toronto Star*, 25 Oct. 2020.

McMurty, Alyssa. "Spain Claims Russian Meddling in Catalan Crisis." *Anadolu Agency*. 13 Nov. 2017, https://www.aa.com.tr/en/europe/spain-claims-russian-meddling-in-catalan-crisis/964432.

"Mikko Kinnunen Appointed Finland's First Ambassador for Hybrid Affairs." Ministry for Foreign Affairs, https://um.fi/press-releases/-/asset_publisher/ued5t2wDmr1C/content/suomen-ensimmaiseksi-hybridisuurlahettilaaksi-mikko-kinnunen. Accessed 7 Mar. 2022.

Miles, Matthew B., et al. *Qualitative Data Analysis: A Methods Sourcebook.* Fourth edition, SAGE, 2020.

Milne, Richard. "Finland Insists on Its Right to Join Nato in Defiance of Russia." *Financial Times*, 2 Jan. 2022, https://www.ft.com/content/28e104d4-bee1-4685-acd1-ff7cd0186ddf.

Milner, Helen V., and Dustin Tingley. *Sailing the Water's Edge: The Domestic Politics of American Foreign Policy*. Princeton University Press, 2015.

Minder, Raphael. "Catalan Separatist Leaders Get Lengthy Prison Terms for Sedition." *The New York Times*, 14 Oct. 2019. https://www.nytimes.com/2019/10/14/world/europe/catalonia-separatists-verdict-spain.html.

Molinaro, Bradley P. Moss, Joanne. "The Sanctioning of Trump's Lawyers Is Exactly What Is Supposed to Happen." *The Atlantic*, 28 Aug. 2021, https://www.theatlantic.com/ideas/archive/2021/08/trumps-lawyers-kraken/619915/.

Monsees, Linda. "'A War against Truth' - Understanding the Fake News Controversy." *Critical Studies on Security*, vol. 8, no. 2, May 2020, pp. 116–29.

Nance, Malcolm W., and Rob Reiner. *The Plot to Destroy Democracy: How Putin and His Spies Are Undermining America and Dismantling the West*. First edition, Hachette Books, 2018.

NATO Strategic Communications Centre of Excellence. "About NATO StratCom COE". https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5. Accessed 15 Nov. 2021.

Neiwert, David A. *Alt-America: The Rise of the Radical Right in the Age of Trump*. Verso, 2017.

Nenye, Vesa, et al. *Finland at War: The Winter War 1939-40*. 2018.

Niglia, A. *Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges*. IOS Press, Incorporated, 2016.

Nimmo, Ben, et al. *Secondary Infektion*. Graphika, 2020, https://secondaryinfektion.org/.

Nordlinger, Jay. "'Falsehood Flies, and Truth Comes Limping After It.'" *National Review*, 1 Oct. 2020, https://www.nationalreview.com/magazine/2020/10/19/falsehood-flies-and-truth-comes-limping-after-it/.

Nyberg, René. "Hybrid Operations and the Importance of Resilience: Lessons From Recent Finnish History." *Carnegie Endowment for International Peace*, https://carnegieendowment.org/2018/02/08/hybrid-operations-and-importance-of-resilience-lessons-from-recent-finnish-history-pub-75490. Accessed 9 Feb. 2022.

Ong, Jonathan Corpus, and Jason Vincent Cabanes. "Politics and Profit in the Fake News Factory." NATO Strategic Communications Centre of Excellence, 2019.

Palmer, Angela-Gabrielle, and Christopher Norman. "AfD's Manipulation Campaign."

The Governance Post, 17 Dec. 2017, https://www.hertie-school.org/the-governance-post/2017/12/afds-manipulation-campaign-fake-news-botnets-foreign-influences/.

Peters, Michael A. "The Information Wars, Fake News and the End of Globalisation." *Educational Philosophy and Theory*, vol. 50, no. 13, Jun. 2018, pp. 1161-1164.

Pherson, Randolph H., et al. "Strategies for Combating the Scourge of Digital Disinformation." *International Journal of Intelligence and CounterIntelligence*, vol. 34, no. 2, Apr. 2021, pp. 316–41.

Pogue, James. "What Peter Thiel, J.D. Vance, and Others Are Learning From Curtis Yarvin and the New Right." *Vanity Fair*. 20 Apr. 2022, https://www.vanityfair.com/news/2022/04/inside-the-new-right-where-peter-thiel-is-placing-his-biggest-bets.

Polyakova, Alina, and Spencer P. Boyer. "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition." *Brookings*. Mar. 2018.

Polyakova, Alina, and Daniel Fried. "Democratic Offense against Disinformation." *The Atlantic Council Digital Forensic Research Lab*, https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-offense-against-disinformation/. Accessed 23 Feb. 2022.

Pomerantsev, Peter. *This Is Not Propaganda: Adventures in the War against Reality*. First Edition, PublicAffairs, 2019.

Pomerantsev, Peter, and Michael Weiss. "How the Kremlin Weaponizes Information, Culture and Money." *Institute of Modern Russia*, 2014.

---. Russia and the Menace of Unreality: How Vladimir Putin Is Revolutionizing Information Warfare. *The Atlantic*, Sept. 2014, https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/.

Pomerleau, Mark. "United States Military Conducted 2 Dozen Cyber Operations to Head off 2020 Election Meddling." *C4ISRNET*, 25 Mar. 2021, https://www.c4isrnet.com/cyber/2021/03/25/us-military-conducted-2-dozen-cyber-operations-to-head-off-2020-election-meddling/.

"Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for United States National Security. Minority Staff Report, 115–21," *United States Senate Committee on Foreign Relations*, 10 Jan. 2018, p. 206.

Pynnöniemi, Katri. "The Asymmetric Approach in Russian Security Strategy: Implications for the Nordic Countries." *Terrorism and Political Violence*, vol. 31, no.

1, Jan. 2019, pp. 154–67.

Pynnöniemi, Katri, and András Rácz, editors. *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine.* Ulkopoliittinen Instituutti, 2016.

Pynnöniemi, Katri, and Sinikukka Saari. "NATO Review - Hybrid Influence – Lessons from Finland." *NATO Review*, 28 June 2017, https://www.nato.int/docu/review/articles/2017/06/28/hybrid-influence-lessons-from-finland/index.html.

Radin, Andrew, et al. "Understanding Russian Subversion: Patterns, Threats, and Responses." *RAND Corporation*, 2020.

Ravitch, Sharon M., and Nicole Mittenfelner Carl. *Qualitative Research: Bridging the Conceptual, Theoretical, and Methodological*. Second edition, Sage, 2021.

Reardon, Robert J. "Article Review 122 on 'The Power of Nations: Measuring What Matters.'" *H-Diplo | ISSF*, 18 July 2019, https://issforum.org/articlereviews/122-measuring.

"Relations with Finland." *North Atlantic Treaty Organization*, 2 Sept. 2021, https://www.nato.int/cps/en/natohq/topics_49594.htm.

Richey, Mason. "Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation." *Asia Europe Journal*, vol. 16, no. 1, Mar. 2018, pp. 101–13.

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux, 2020.

Riehle, Kevin P. "Winners and Losers in Russia's Information War." *Intelligence and National Security*, Jan. 2021, pp. 1–8.

Rodríguez-Virgili, Jordi, et al. "Digital Disinformation and Preventive Actions: Perceptions of Users from Argentina, Chile, and Spain." *Media and Communication*, vol. 9, no. 1, Mar. 2021, pp. 323–37.

Rosenberger, Laura. "Disinformation Disorientation." *Journal of Democracy*, vol. 31, no. 1, 2020, pp. 203–07.

Rosenberger, Laura, and Bradley Hanlon. "Countering Information Operations Demands A Common Democratic Strategy." *The German Marshal Fund of the United States*. 2019. https://securingdemocracy.gmfus.org/countering-information-operations-demands-a-common-democratic-strategy/

Ruggie, John Gerard. "International Regimes, Transactions, and Change: Embedded

Liberalism in the Postwar Economic Order." *International Organization*, 1982, pp. 195-231.

Rusi, Alpo. “The Cold War History of Finland in Perspective - Research of Finlandisation or Not?” 12 May 2017, http://www.alporusi.fi/1/post/2017/12/the-cold-war-history-of-finland-in-perspective-research-of-finlandisation-or-not.html.

“Russian Active Measures Campaigns and Interference in the 2016 United States Election, Volumes I-V. 116–290,” *United States Senate Select Committee on Intelligence*, Oct. 2019, https://www.congress.gov/congressional-report/116th-congress/senate-report/290/1?s=1&r=50.

Sahay, Usha. “Revitalizing NATO: A Role for the United States Congress,” *Belfer Center for Science and International Affairs*. https://www.belfercenter.org/publication/revitalizing-nato-role-us-congress. Accessed 23 Feb. 2022.

Satariano, Adam, and Amie Tsang. “Who’s Spreading Disinformation in U.K. Election? You Might Be Surprised.” *The New York Times*, 10 Dec. 2019. https://www.nytimes.com/2019/12/10/world/europe/elections-disinformation-social-media.html.

Saurwein, Florian, and Charlotte Spencer-Smith. “Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe.” *Digital Journalism*, vol. 8, no. 6, July 2020, pp. 820–41.

Schia, Niels Nagelhus, and Lars Gjesvik. “Hacking Democracy: Managing Influence Campaigns and Disinformation in the Digital Age.” *Journal of Cyber Policy*, vol. 5, no. 3, Sept. 2020, pp. 413–28.

“Security Strategy for Society – Turvallisuuskomitea.” *The Security Committee, Government of Finland*, 2 Nov. 2017, www.turvallisuuskomitea.fi/en.

Shaw, Christopher. “The Topography of Geopolitics: Net Resources and the Past, Present, and Future of American Power,” *RealClearDefense*. 10 Sept. 2021, https://www.realcleardefense.com/articles/2021/09/09/the_topography_of_geopolitics_net_resources_and_the_past_present_and_future_of_american_power_793862.html.

Sheives, Kevin. “How to Support a Globally Connected Counter-Disinformation Network - War on the Rocks.” *War on the Rocks*, 20 Jan. 2022, https://warontherocks.com/2022/01/how-to-support-a-globally-connected-counter-disinformation-network/.

Singer, J. David. 1987. "Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816-1985" *International Interactions*, 14: 115-32.

Snyder, Timothy. *On Tyranny: Twenty Lessons from the Twentieth Century*. First edition, Tim Duggan Books, 2017.

---. "The American Abyss." *The New York Times*, 9 Jan. 2021, https://www.nytimes.com/2021/01/09/magazine/trump-coup.html.

Splidsboel Hansen, Flemming. "Russian Hybrid Warfare: A Study of Desinformation." *Danish Institute for International Studies*, 2017.

Šramková, Vanesa. "Forming the EU Disinformation Policy." 29 Sept. 2018, https://is.cuni.cz/studium/dipl_st/index.php?do=main&doo=detail&did=205720.

Standish, Reid. "Why Is Finland Able to Fend Off Putin's Information War?" *Foreign Policy*, 1 Mar. 2017, https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.

Stanley, Jason. *How Fascism Works: The Politics of United States and Them*. Random House trade paperback edition, Random House, 2020.

Stelzenmüller, Constanze. "The Impact of Russian Interference on Germany's 2017 Elections." Brookings Institution. 28 Jun. 2017.

Stengel, Richard. *Information Wars: How We Lost the Global Battle against Disinformation & What We Can Do about It*. First edition, Atlantic Monthly Press, 2019.

Stoker, Donald J. *Why America Loses Wars: Limited War and United States Strategy from the Korean War to the Present*. Cambridge University Press, 2019.

Sukhankin, Sergey. "COVID-19 as a Tool of Information Confrontation: Russia's Approach," *The School of Public Policy Publications*, vol. 13, no. 3, Apr. 2020.

---. "The Western Alliance in the Face of the Russian (Dis)Information Machine: Where Does Canada Stand?" *Canadian Global Affairs Institute*, 2019.

Sultan, Oz. "Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s." *The Cyber Defense Review*, vol. 4, no. 1, 2019, pp. 43–60.

Swisher, Kara. "Putin Will Not Lose. He's Not Going to Let That Happen." *The New York Times*, 7 Mar. 2022. https://www.nytimes.com/2022/03/07/opinion/sway-kara-swisher-clint-watts.html.

Szymański, Piotr. "With Russia Right across the Border: Finland's Security Policy." *Ośrodek Studiów Wschodnich*, May 2018.

Taylor, Margaret. "Combating Disinformation and Foreign Interference in Democracies:

Lessons from Europe." Brookings Institution. 31 Jul. 2019. https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/.

Tenold, Vegas. *Everything You Love Will Burn: Inside the Rebirth of White Nationalism in America*. First edition, Nation Books, 2018.

Tenove, Chris. "Protecting Democracy from Disinformation: Normative Threats and Policy Responses." *The International Journal of Press/Politics*, vol. 25, no. 3, July 2020, pp. 517–37.

"The Disinformation Station Germany Fears Influence of Russian Propaganda Channel." *Yerepouni Daily News*, 4 Mar. 2021.

Theohary, Catherine. "Defense Primer: Information Operations." *Congressional Research Service*, 1 Dec. 2021, https://sgp.fas.org/crs/natsec/IF10771.pdf.

Thomas, Matthew. "Defeating Disinformation Threats." *Foreign Policy Research Institute*, 1 Feb. 2020, https://www.fpri.org/article/2020/02/defeating-disinformation-threats/.

Thomas, Timothy. "Thinking Like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War." *Foreign Military Studies Office*, Fort Leavenworth, Kansas, 2016.

Thompson, Stuart A. "How Russian Media Uses Fox News to Make Its Case." *The New York Times*, 15 Apr. 2022. https://www.nytimes.com/2022/04/15/technology/russia-media-fox-news.html.

Tiido, Anna. "Russians in Europe: Nobody's Tool." *Estonian Foreign Policy Institute*, Sep. 2019.

Trotter, William R. *A Frozen Hell: The Russo-Finnish Winter War of 1939-40*. Algonquin Books of Chapel HIll, 1991.

Tsurkan, Anna. "Elections in Canada and Russia in 2019: A Comparative Analysis of Cross-National Media Coverage." *Canadian Journal of European and Russian Studies*, vol. 14, no. 1, Apr. 2021, pp. 55–78.

Tucker, Patrick. "Russian Trolls Are Hammering Away at NATO's Presence in Lithuania." *Defense One*, 3 Dec. 2019, https://www.defenseone.com/technology/2019/12/russian-trolls-are-hammering-away-natos-presence-lithuania/161654/.

"Undermining Democratic Institutions and Splintering NATO: Russian Disinformation Aims." *House of Representatives Committee on Foreign Affairs*, 9 Mar. 2017,

https://foreignaffairs.house.gov/2017/3/undermining-democratic-institutions-and-splintering-nato-russian-disinformation.

United States Marine Corps. Marine Corps Doctrinal Publication 1: Warfighting. United States Marine Corps, 1997.

Vandiver, John. "SACEUR: Allies Must Prepare for Russia 'Hybrid War.'" *Stripes.Com*, 4 Sep. 2014.

Vilmer, Jean-Baptiste Jeangène. *The "Macron Leaks" Operation: A Post-Mortem*, Atlantic Council, 2019

Vilmer, Jean-Baptiste Jeangène, and Paul Charon. "Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare." *WarOnTheRocks.com*, 21 Jan. 2020.

Vindman, Alexander. *Here, Right Matters: An American Story*. 2021.

Vo, Nguyen, and Kyumin Lee. "Standing on the Shoulders of Guardians: Novel Methodologies to Combat Fake News." *Disinformation, Misinformation, and Fake News in Social Media*, edited by Kai Shu et al., Springer International Publishing, 2020, pp. 183–210.

Voo, Julia, et al. *National Cyber Power Index 2020*. Sep. 2020. https://www.belfercenter.org/publication/national-cyber-power-index-2020

Wagnsson, Charlotte. "What Is at Stake in the Information Sphere? Anxieties about Malign Information Influence among Ordinary Swedes." *European Security*, vol. 29, no. 4, Oct. 2020, pp. 397–415.

Wagnsson, Charlotte, and Maria Hellman. "Normative Power Europe Caving In? EU under Pressure of Russian Information Warfare: Normative Power Europe Caving In?" *JCMS: Journal of Common Market Studies*, vol. 56, no. 5, July 2018, pp. 1161–77.

Walter, Barbara F. *How Civil Wars Start*. First Edition, Crown, 2022.

Wardle, Claire, and Hossein Derakhshan. "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making." *Council of Europe*, 26 Oct. 2017.

"Warsaw Institute Debate: Information Warfare and Activities of Special Services." *Warsaw Institute*, 13 Dec. 2018, https://warsawinstitute.org/warsaw-institute-debate-information-warfare-activities-special-services/.

Weiss, Andrew S., "With Friends Like These: The Kremlin's Far-Right and Populist

Connections in Italy and Austria." *Carnegie Endowment for International Peace*, 2020, https://carnegieendowment.org/2020/02/27/with-friends-like-these-kremlin-s-far-right-and-populist-connections-in-italy-and-austria-pub-81100.

Wigell, Mikael. "Democratic Deterrence: How to Dissuade Hybrid Interference." *The Washington Quarterly*, vol. 44, no. 1, Jan. 2021, pp. 49–67.

Wood, Steve. "'Understanding' for Russia in Germany: International Triangle Meets Domestic Politics." *Cambridge Review of International Affairs*, Jan. 2020, pp. 1–24.

Woodruff Swan, Betsy, and Bryan Bender. "Spy Chiefs Look to Declassify Intel after Rare Plea from 4-Star Commanders." POLITICO, 26 Apr. 2021, https://www.politico.com/news/2021/04/26/spy-chiefs-information-war-russia-china-484723.

Wylie, J. C. *Military Strategy: A General Theory of Power Control*. Naval Institute Press, 2014.