

**How Do Authoritarian States React When Targeted by the Use of Information
as a Foreign Policy Tool? Case Studies of Russia and North Korea**

by

Scott Fisher

A Dissertation submitted to the
Graduate School-Newark
Rutgers, The State University of New Jersey
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy
Graduate Program in Global Affairs
written under the direction of
Dr. Norman Samuels
and approved by

Newark, New Jersey

October, 2018

Copyright

© 2018

Scott Fisher

ALL RIGHTS RESERVED

ABSTRACT OF THE DISSERTATION

**How Do Authoritarian States React When Targeted by the Use of Information
as a Foreign Policy Tool? Case Studies of Russia and North Korea**

By Scott Fisher

Dissertation Director:
Dr. Norman Samuels

Using sentiment analysis of government media and case studies of North Korea and Russia as proxies for authoritarian states attempting to control their domestic information environment, this research demonstrates that information tools capable of threatening that control produce a consistently negative reaction at least equal to the more common diplomatic, economic, and military tools of statecraft.

Acknowledgement

For Marisa – meeting you was the best thing that ever happened to me.

Table of Contents

CHAPTER ONE

Introduction	1
Research Question	3
Definitions	4
Proposed Methodology	9
Conclusion	12

CHAPTER TWO

Literature Review	14
This Research	19
IR Approaches	24
Communications and Media Studies	36
History and Background	44
DIME	50
Russia	53
North Korea	55
Digital Humanities	57
Conclusion	58

CHAPTER THREE

Research Methodology **60**

Media Sources	61
Key Events	62
Event Analysis and Digital Humanities	64
GDELT	72
Additional Tools for Data Collection and Analysis	75
Conclusion	79

CHAPTER FOUR

Russia **82**

Data Collection	84
<u>Section 1</u> : TASS and MOFA	86
Overview	88
Negative Sentiment	89
Positive Sentiment	99
TASS and MOFA Conclusion	113
<u>Section 2</u> : GDELT	114
Military	117
Economic	123
Diplomacy	130
Information	134
GDELT Conclusion	147

Overall Conclusion	149
--------------------------	-----

CHAPTER FIVE

North Korea 153

Research Method	159
-----------------------	-----

Sources	162
---------------	-----

Data Collection	163
-----------------------	-----

<u>Section 1</u> : KCNA, Rodong Sinmun, Uriminzokkiri	165
---	-----

Rodong Sinmun Military	166
-----------------------------------	-----

Economic	168
----------------	-----

Diplomatic	169
------------------	-----

Information	170
-------------------	-----

Uriminzokkiri	172
---------------------	-----

Military	174
----------------	-----

Economic	176
----------------	-----

Diplomacy	177
-----------------	-----

Information	178
-------------------	-----

KCNA	180
------------	-----

Military	183
----------------	-----

Economic	189
----------------	-----

Diplomatic	190
------------------	-----

Information	198
-------------------	-----

Conclusion	202
Twitter Data	203
Actions	205
Conclusion	213
 CHAPTER SIX	
Conclusion	216
Technical Notes	217
Policy Recommendations	220
 Bibliography	 224

List of Tables

Table 1 – Event list and sentiment analysis for Russia	108
--	-----

List of Illustrations

Figure 1: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016	70
Figure 2: TASS reporting on Freedom House	91
Figure 3: TASS reporting on Freedom House, 2013-2016	92
Figure 4: TASS reporting on U.S. economic sanctions in December 2015	94
Figure 5: Timeline of TASS reporting on U.S. economic sanctions in Dec. 2015	95
Figure 6: Russian government views of the U.S. government from 2007-16	97
Figure 7: Russian government sentiment toward the U.S. government, 1 January 2009 to 30 September 2016	98
Figure 8: TASS reporting on NATO's Trident Exercises	101
Figure 9: MOFA's largely positive response to the U.S. decision to base anti-missile defenses in Eastern Europe	102
Figure 10: MOFA's reaction to the Baltic states (Estonia, Latvia, Lithuania) joining NATO in 2004	103
Figure 11: Timeline showing MOFA sentiment toward NATO expansion into the three Baltic states in 2004	104
Figure 12: MOFA's sentiment toward NATO exercises, 2010-2016	105
Figure 13: Note the sudden, sharp decrease in MOFA commentary on NATO exercises beginning in the spring of 2014	106
Figure 14: MOFA's sentiment toward NATO naval vessels entering the Black Sea during the conflict with Georgia in August 2008	107
Figure 15: Overall MOFA Tweet Sentiment	109
Figure 26: Russian MOFA sentiment 06-2017 to 01-2018 – ‘sanction’	110
Figure 17: Russian MOFA sentiment 06-2017 to 01-2018 – ‘NATO’	111

Figure 18: Russian MOFA sentiment 06-2017 to 01-2018 – ‘zapad’	111
Figure 19: Russian government sentiment toward the U.S. government	115
Figure 20: U.S. government military threats and actions toward the Russian government, broadly categorized	117
Figure 21: U.S. government military threats toward the Russian government	119
Figure 22: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016	120
Figure 23: U.S. government economic threats and actions toward the Russian government, broadly categorized	124
Figure 24: U.S. government economic threats and actions toward the Russian government	125
Figure 25: U.S. government economic threats and actions toward Russia, not just the Russian government	127
Figure 26: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016	129
Figure 27: U.S. government diplomatic threats and actions toward the Russian government, broadly categorized	131
Figure 28: U.S. government diplomatic threats and actions toward the Russian government	132
Figure 29: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016	133
Figure 30: U.S. government information threats and actions toward the Russian government, broadly defined	136
Figure 31: U.S. government information threats and actions toward the Russian government	137
Figure 32: U.S. government information-based threats and actions toward Russia, not just the Russian government	138

Figure 33: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016	139
Figure 34: Russian government actions and sentiment toward the Russian media and political opposition	141
Figure 35: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016	142
Figure 36: U.S. government economic threats toward the Russian government	144
Figure 37: U.S. government information threats toward the Russian government	144
Figure 38: U.S. government diplomatic threats toward the Russian government	145
Figure 39: U.S. government military threats toward the Russian government	146
Figure 40: Russian government actions and sentiment toward the Russian media and political opposition	146
Figure 41: Rodong Sinmun - 'Ulji'	167
Figure 42: Rodong Sinmun - 'Foal'	167
Figure 43: Rodong Sinmun - 'Military Exercises'	168
Figure 44: Rodong Sinmun - 'sanctions'	169
Figure 45: Rodong Sinmun - '2270'	170
Figure 46: Rodong Sinmun - 'psychological warfare'	171
Figure 47: Rodong Sinmun - 'loudspeaker'	172
Figure 48: All Uriminzokkiri Reporting Feb 2015 - Aug 2017	173
Figure 49: 2015-2017 Uriminzokkiri - 'military exercise'	174
Figure 50: 2015-2017 Uriminzokkiri - 'Ulji'	175

Figure 51: 2015-2017 Uriminzokkiri – ‘foal’	176
Figure 52: 2015-2017 Uriminzokkiri – ‘sanctions’	177
Figure 53: 2015-2017 Uriminzokkiri – UN resolutions ‘2270’, ‘2321’ and ‘2371’	178
Figure 54: 2015-2017 Uriminzokkiri – ‘loudspeaker’	179
Figure 55: 2015-2017 Uriminzokkiri – ‘psychological warfare’	179
Figure 56: All KCNA Reporting from Jan 2002 to Aug 2017	181
Figure 57: Polarity of KCNA Reporting by Month, Jan 2002 to Aug 2017	182
Figure 58: KCNA Reporting, Percent Difference with Previous Month	183
Figure 59: 2002-2017 KCNA – ‘military exercise’	184
Figure 60: 2002-2017 KCNA – ‘ulji’	185
Figure 61: 2002-2017 KCNA – ‘foal’	185
Figure 62: 2002-2017 KCNA Monthly Aggregate Sentiment	187
Figure 63: 2002-2017 KCNA – ‘sanction’	190
Figure 64: 2002-2017 KCNA – Combined UNSC Resolutions	191
Figure 65: 2002-2017 KCNA – Combined UNSC Resolutions Timeline	192
Figure 66: 2002-2017 KCNA – UNSC 1718	193
Figure 67: 2002-2017 KCNA – UNSC 1874	194
Figure 68: 2002-2017 KCNA – UNSC 2087	195
Figure 69: 2002-2017 KCNA – UNSC 2270	196
Figure 70: 2002-2017 KCNA – UNSC 2371	197
Figure 71: 2002-2017 KCNA – ‘Psychological Warfare’	199

Figure 72: 2002-2017 KCNA – ‘loudspeaker’	200
Figure 73: 2002-2017 KCNA – ‘leaflet’	200
Figure 74: 2002-2017 KCNA – ‘Psychological Warfare’ Timeline	201
Figure 75: 2002-2017 KCNA – ‘leaflet’ Timeline	202
Figure 76: Beyond Parallel Kinetic Incident Database, 01-2002 to 08-2017	206
Figure 77: Beyond Parallel Kinetic Incident by Type	207
Figure 78: Beyond Parallel Kinetic Incident by Type	211

Chapter One: Introduction

In 1971, when South Africa was debating whether to allow television into the country, a former Minister of Posts and Telegraphs, “rejected it as a symbol of Western degeneracy that ‘would lead to the demoralization of South African civilization and the destruction of apartheid.’ He turned out to be right.”¹

Throughout the Cold War, in an effort to control the underground ‘samizdat’ press (censored materials reproduced and distributed by hand), the former Soviet Union went so far as to restrict access to copy machines.² This was in addition to jamming radio and TV frequencies used by outside broadcasters like the BBC and Voice of America.

In 1994, “Iran’s highest-ranking cleric issued a fatwa against satellite television dishes because they would introduce a cheap alien culture and spread the moral diseases of the West. He also turned out to be correct. A decade later, mass demonstrations in Tehran followed the spread of private American TV broadcasts,” from Iran’s diaspora in Los Angeles, broadcasting previously unavailable commentary and coverage of Iran’s politics 24 hours a day.³

During the Arab Spring of 2011, in January, the Egyptian government first blocked whole websites, including Facebook and Twitter, before finally shutting down mobile service and the country’s access to the internet entirely in late

¹ Nye, Jr., *Soft Power: The Means to Success in World Politics*, pg. 51.

² For more on Soviet history and regulation of photocopiers and the samizdat press, please see Soldatov, Andrei, and Irina Borogan. *The Red Web: The Struggle between Russia’s Digital Dictators and the New Online Revolutionaries*. 2015, pgs. 3-23.

³ Nye, Jr., *Soft Power: The Means to Success in World Politics*, pg. 51.

January.^{4 5} Outside the region, China and North Korea simply banned and censored all mention of 'Arab Spring' and related terms from their domestic information environments. Though the information control techniques worked in North Korea, China, and some parts of the Arab world, they were less successful in Egypt and Syria.

In 2015, North Korean soldiers planted landmines on the southern side of the border in an area where South Korean soldiers were known to patrol, eventually maiming two South Korean soldiers. "South Korea retaliated with a measure that they thought was equally, if not more, damaging to North Korea's morale than maiming two soldiers: turning on loudspeakers [that penetrated miles into the North.] North Korea's top negotiator called South Korea's actions of turning on their loudspeakers a 'declaration of war.' His colleague, North Korea's deputy permanent representative to the United Nations, called the broadcasts 'psychological warfare.'" A former North Korean propaganda official said the broadcasts, "are akin to a peaceful version of the nuclear bomb."⁶ But it worked, within two weeks the South had received an exceedingly rare 'expression of regret' from the North.

And then Seoul turned off the speakers.

A random collection of anecdotes? Or demonstrations of the power of information tools to threaten (or produce) change in the behavior of authoritarian states?

⁴ Dunn, "Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising."

⁵ Cornell University Library, The January 25 Revolution.

⁶ Baek, Jieun. *North Korea's Hidden Revolution: How the Information Underground Is Transforming a Closed Society*, pgs. 187-188.

Or do such demonstrations even matter? If the leaders of authoritarian states believe, or react as if they believe, the spread of unfiltered, uncensored information is a threat, has not an effect been achieved? For if an authoritarian leader views information as a threat, and an outside actor takes advantage of that view by using, or threatening to use, information tools in order to affect, influence, or secure an agreement with that targeted state, has not a policy goal been achieved through the use, or threatened use, of information? Like the threatened or actual employment of economic sanctions as a tool of foreign policy, information tools also offer multiple options for operationalization: threatening implementation, implementation, offering to rescind measures in place, and actually rescinding those measures. While hardly unique to information tools, these implementation steps offer negotiators added flexibility in attempting to achieve their goals with the targeted authoritarian state.

Research Question

Anecdotes aside, do authoritarian states actually view information as a threat? If so, how do threats in the information environment compare to diplomatic, economic, and military threats? Finally, do states with the tightest controls over information take a threat to those controls more seriously than states with relatively fewer controls? Answering all three of these questions benefits from a rephrasing into one central question: in terms of authoritarian states, how does the outside use of information as a foreign policy tool to threaten or pressure a regime compare to the use of diplomatic, military, and economic tools? Once this question is

answered, for multiple states, the paper can demonstrate whether authoritarian states actually view information as a threat, how that threat compares to more common foreign policy pressure tools (e.g. economic sanctions, diplomatic resolutions, military threats), and by researching two countries with different levels of information controls, provide an initial finding as to whether regimes with tighter controls react more strongly than states with relatively fewer controls.

The research here addresses these questions by analyzing both state actions and official state media reporting in response to an outside actor's actions or comments in the four categories of policy tools: diplomatic, informational, military, and economic. The operating hypothesis is that the more controlling a government is of its domestic information environment, the more negatively it will react to having that control challenged. It is important to note here at the outset that the specific message, content, and narrative is not under investigation; the research focus is the control countries exercise over information flows and how they react when these controls are threatened, attacked, or disabled by an outside actor.

Also noted here at the start, and discussed in more detail later in the paper, is that cyberspace is considered part of the wider information environment. Thus, information as a foreign policy tool explicitly includes cyberspace and cyber tools.

Definitions

With a goal of finding definitions understood across both academic and practitioner realms, this paper largely bases key definitions on those from NATO governments and militaries and private sector organizations like Freedom House

and Facebook. Future research comparing/contrasting U.S. and NATO definitions with those from Russia, China, and other countries would likely make for a utile, interesting paper.

Incumbent on research into authoritarian states is a working definition of *authoritarian*. While the United Nations and international law provide definitions of *democracy* (e.g. the Universal Declaration of Human Rights,⁷ the International Covenant on Civil and Political Rights,⁸ the UN World Summit of 2005⁹), similar internationally agreed upon definitions of *authoritarian* are lacking. For our purposes, especially given the research focus on states and information access, we will define *authoritarian* (whether traditional¹⁰ or modern¹¹) as states that either directly (e.g. North Korea) or indirectly (e.g. Russia, “through state enterprises and oligarchic cronies”¹²) restrict citizens’ access to information to the extent they rank at or near the bottom on standard international measures of press and/or information freedom.^{13 14 15 16} We select international, comparative rankings as the basis of our definition in order to test/measure whether states most restrictive of their domestic information environment react more strongly to challenges to that

⁷ UN, *Universal Declaration of Human Rights*. United Nations, 1948.

⁸ UN General Assembly. *International Covenant on Civil and Political Rights*. United Nations, 1966.

⁹ UN. *Democracy*. United Nations.

¹⁰ Puddington, Arch. *Breaking Down Democracy: Goals, Strategies, and Methods of Modern Authoritarians*, pg. 5.

¹¹ Puddington, Arch. *Breaking Down Democracy: Goals, Strategies, and Methods of Modern Authoritarians*, pg. 6.

¹² Puddington, Arch. *Breaking Down Democracy: Goals, Strategies, and Methods of Modern Authoritarians*, pg. 6.

¹³ Freedom House, *Freedom in the World 2017*, Washington, DC: Freedom House.

¹⁴ Reporters Without Borders, *2017 World Press Freedom Index*, Paris: Reporters Without Borders.

¹⁵ Freedom House, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*, Washington, DC: Freedom House.

¹⁶ Freedom House, *Freedom of the Press 2017: Press Freedom’s Dark Horizon*, Washington, DC: Freedom House.

control than comparatively less-restrictive states. We will examine these rankings in greater detail in the respective research chapters on Russia and North Korea.

The U.S. Department of Defense (DoD) defines the *information environment* as, “The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.”¹⁷ NATO’s definition of the term is similarly broad, “The virtual and physical space in which information is received, processed and conveyed. It consists of the information itself and information systems.”¹⁸ The broader nature of the information environment compared to cyberspace is the reason we chose to use that phrase here – it allows for research into states like North Korea that largely prevent their citizens from accessing cyberspace (outside of a domestic-only intranet), but who still exist in the wider information environment of broadcasts, printed materials, and even mobile communications technologies.

The U.S. DoD defines *cyberspace* as, “A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”¹⁹ The reader will note the explicit statement that cyberspace lies within the overall information environment. This is perhaps the key definitional concept of this paper

¹⁷ U.S. Joint Publication 3-13, *Information Operations*, 20 November 2014, pg. GL-3.

¹⁸ NATO. “AJP-3.10 Allied Joint Doctrine for Information Operations.” NATO Standardization Agency, November 2009, pg. Lexicon-6.

¹⁹ U.S. Joint Staff Joint Publication 3-12 (R), *Cyberspace Operations*, 5 February 2013, pg. GL-4.

– the specific inclusion of both cyberspace tools and older information tools (from print to radio and TV) as part of the information environment.

A common term broadly related to our topic is *propaganda*. The term has such negative connotations that the U.S., by doctrine, defines it as *adversary* messaging. “Any form of adversary communication, especially of a biased or misleading nature, designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly.”²⁰ It is important to draw a distinct line here between our research, which focuses on the ability to access information, and terms like *propaganda* that emphasize the promulgation of a specific narrative or piece of information.

Information operations (IO) is defined by the DoD as, “The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.”²¹ NATO’s definition of IO is similar, though features less of a laundry-list of activities, “NATO military advice and co-ordination of military information activities in order to create desired effects on the will, understanding, and capabilities of adversaries and other NAC-approved parties in support of Alliance operations, missions and objectives.”²²

²⁰ U.S. Joint Publication 3-13.2, *Military Information Support Operations*, Joint Publication 3-13.2, U.S. Joint Chiefs of Staff, 2010.

²¹ U.S. Army Field Manual 3-13, *Inform and Influence Activities*, pg. Glossary-2.

²² NATO Strategic Communications Centre of Excellence, *About Strategic Communications*, <http://www.stratcomcoe.org/about-strategic-communications>, accessed 13 July 2016.

From the private sector, Facebook defines information operations as, “actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts aimed at manipulating public opinion (we refer to these as “false amplifiers”).”²³

An alternative definition courtesy of academia describes IO as, “a formal attempt by the U.S. government to develop a set of doctrinal approaches for its military and diplomatic forces to use and operationalize the power of information.”²⁴ The broader private sector (Facebook) and academic (minus the U.S. government focus) definitions are the most useful for our research and the ones we will broadly utilize to describe the use of information as a tool of foreign policy and national security by a state or non-state actor.

From this list of definitions, we can see that the U.S. government has no shortage of committees writing manuals. Also apparent is that our proposed research encompasses a number of these terms, with the broadest, academic definition of *information operations* coming the closest to describing our research into the use of information access, rather than narrative, as a foreign policy tool.

Where appropriate, we will apply these terms in the paper, under the definitional framework provided here. The intention of the shared definitions is to allow for a clearer discussion of often-misunderstood concepts and to increase the

²³ Weedon, et al., “Information Operations and Facebook.” pg. 4.

²⁴ Armistead, Leigh. *Information Operations Matters*, pg. 24.

policy relevance of the paper by incorporating terms already familiar to national security and foreign policy practitioners from around the world.

Proposed Methodology

A mixed-methods approach is proposed, including a qualitative look at the countries and governments involved, followed by a quantitative approach to determine how negatively countries react when their information controls are attacked or threatened. Finally, a comparative approach will be taken, involving both qualitative and quantitative findings, to determine how information tools compare to the more common diplomatic, economic, and military tools of statecraft.

In terms of data, the Korean peninsula provides our most crucial dataset. With research access to North Korea limited (as a 'traditional authoritarian' the North maintains an isolated, autarchic relationship with the outside world), one of the few means available for gaining insight into the regime is monitoring state-controlled media, primarily the *Korean Central News Agency* (the country's official news media organization) and the *Rodong Shinmun* (the official newspaper of the North's ruling Labor party). By using official media to track the North's responses to select outside actions (e.g. military exercises, economic sanctions, diplomacy, information campaigns), we can build a database of the North's official reactions to outside foreign policy tools.

Of the two sources mentioned above, the *Korean Central News Agency* (KCNA) is of primary importance since it is the media outlet of record for the North. More problematically for our research, changes in the North's policies or personnel

often result in a culling or altering of previously posted reports on North Korean websites. These changes highlight the importance the North's leadership places on these websites as the regime's official narrative, including, in addition to Korean, English, Spanish, and occasionally Russian and Japanese.

At the other end of the spectrum, in Russia, the media and information environments are decidedly more complex. However, much of the media still comes under state control, with independent organizations like *Reporters Without Borders* and *Freedom House* reporting a growing loss of independent media outlets in the country. By using the traditional official Russian media outlet *TASS*, as well as official regime commentary from the Ministry of Foreign Affairs, to create a database of Russia responses to outside activities, we can gain insight into Moscow's views on the threats posed by decreased control over its domestic information environment, again as compared to its views on economic, diplomatic, and military actions/threats.

By overlapping events (e.g. a South Korean group sending leaflets into North Korea, or international calls for press freedom in Russia) with reactions published in official state media, as expressed through the databases of regime reporting discussed above, we can analyze how these countries react to outside information campaigns that threaten or pierce this control. The findings can then be compared to official reactions to other foreign policy tools (i.e. economic sanctions, diplomatic campaigns, military actions). The overall and comparative results should provide evidence of whether and how much information campaigns are viewed as a threat by these governments. Should they be viewed as a threat, we can then begin to

assess whether they carry a deterrence value and, if so, how information can be added to the existing foreign policy toolkit of diplomatic, economic, and military capabilities.

Our research will focus on Russia and North Korea as authoritarian outliers on the range of least-most restrictive domestic information environments, respectively, as per rankings maintained by Freedom House and others. If our data and analysis reveal an effect at either or both ends of the spectrum, we can later apply the methodology and findings to China and Iran, countries closer to the center of this spectrum.

Each research chapter opens with an examination of that country's information environment and related factors. Of the two countries, North Korea will be the most closely examined, due to its much tighter restrictions on the flow of information.

The quantitative aspects of our research will involve a taxonomy and an ontology of North Korean and Russian reactions to threats in the diplomatic, economic, military, and information domains. These reactions will be developed into a database designed to compare the governments' reactions across the four different types of outside pressure. Per above, the operating hypothesis at the start of the research is that the more controlling a government is of its domestic information environment, the more negatively it will react to having that control challenged.

As for other possible research paths, Russian and North Korean officials are deemed unlikely to cooperate with this research. Consequently, no interviews will

be conducted, necessitating no IRB process. Fieldwork is unlikely, since the bulk of this research can be conducted online, including by harnessing VPN (virtual private network) capabilities to make the researcher appear to be accessing any blocked websites (e.g. the KCNA's website in Japan) from within a permitted country.

Related works, including journals, will be surveyed. Due to the nature and immediacy of the topic (e.g. Russia's efforts to influence the 2016 U.S. elections), many of the field's key actors and researchers publish frequently on blogs and social media. These resources will be incorporated into our research.

More problematically, countries and international organizations (e.g. NATO, the UN) often lack or differ on their definitions and understanding of common terms used in this research (e.g. *cyberspace*, *information environment*, *information war*, etc.). For purposes of clarity, this paper primarily uses NATO definitions of key terms. This is not for ideological reasons, but because these are the most internationally-accepted definitions. This definitional framework should assist the portability and saliency of any findings for the policy/practitioner realm.

Conclusion

The idea that economically advanced, liberal democracies are especially vulnerable in the information environment, especially in cyberspace, has gained broad currency due to these societies' heavy commercial and social reliance on the internet. This paper does not dispute these vulnerabilities; instead this research investigates the counterargument that authoritarian states have their own unique information vulnerabilities that could in turn be exploited by liberal democracies.

Any finding(s) that demonstrates a vulnerability to information by Russia or North Korea would be significant by offering an additional foreign policy tool to outside actors aiming to influence, deter, or punish these states. Any findings that demonstrate only limited or no vulnerability to information will support the existing dominance of economic, diplomatic, and military tools in foreign policy and national security.

Based on preliminary findings, our research begins with the idea that closed, authoritarian states like Russia and North Korea share unique vulnerabilities in their domestic information environment. If further research supports these initial findings, the paper will conclude in the applied realm with recommendations for policymakers. These recommendations will offer methods for incorporating information tools into the foreign policy and national security toolkit, helping to reduce the imbalance in the information environment between open, liberal democracies and their closed or semi-closed state-level peers.

Chapter Two: Literature Review

The importance of exploiting what is now called the information environment has long been a part of U.S. government planning, decision-making, and operations. A crucial early success was Benjamin Franklin's use of a "propaganda" campaign to convince the French to enter the U.S. War of Independence in the 1770s.²⁵ After the War of 1812, Jefferson advocated for information campaigns in Europe to counter the "slanders and falsehoods" of the British press.²⁶ Abraham Lincoln's "overtures to British workingmen to support the Union cause during the Civil War" became so common they "offended" the British Foreign Office.²⁷

In 1917, during World War I, President Wilson went beyond previous ad hoc efforts and ordered the establishment of the *Committee on Public Information*, also known as the *Creel Committee*, after the name of its chairman. Before the committee was disbanded in 1919, it was tasked with helping to influence U.S. public opinion to support the war and to counter foreign attempts to influence U.S. public opinion against the war.²⁸

During World War II, President Roosevelt established the Office of War Information (OWI, June 1942 – September 1945) to influence both U.S. and foreign

²⁵ Elder, Robert E. *Information Machine: The United States Information Agency and American Foreign Policy*, pg. 33.

²⁶ Snyder, Alvin. *Warriors of Disinformation*, 1997, pg. 14.

²⁷ Elder, Robert E. *Information Machine: The United States Information Agency and American Foreign Policy*, pg. 33.

²⁸ Woodrow Wilson: "Executive Order 2594 - Creating Committee on Public Information," April 13, 1917 and Armistead, Leigh, *Information Operations Matters*, pg. 70.

audiences regarding the war.²⁹ This followed the establishment of the Office of the Coordinator of Inter-American Cultural Relations in July 1941. Headed by Nelson Rockefeller, its responsibility became the American information effort in Latin and South America during WWII, specifically, fighting Axis (Germany, Italy, Japan) propaganda aimed at influencing the Americas during the war.³⁰ The Axis powers' lack of success in recruiting new supporters and building an anti-Allies coalition in the Americas is at least partially attributable to these efforts.

After WWII, the information programs underwent funding cuts, were reassigned to the State Department, and, as in the aftermath of previous wars (e.g. WWI's Creel Committee), appeared to be on their way to getting eliminated.³¹ However, U.S. Congressmen "junketing" in Europe in 1947 saw Soviet propaganda efforts firsthand and became "convinced that the people of other countries had to get a better understanding of the United States if they were to withstand the 'aggressive psychological warfare' being conducted against America by the Communists."³² This led to the passage of Public Law 402, which reinvigorated the information capabilities remaining from the war (largely at the State Department) and tasked them with 'selling America' overseas.³³ The North Korean invasion of the South in 1950 led to drastically increased funding for U.S. information efforts, and in combination with the 'red scare' of the early 1950s, culminated in the establishment

²⁹ Armistead, Leigh, *Information Operations Matters*, pg. 70 and Roosevelt, Franklin D: "Executive Order 9182 Establishing the Office of War Information.," June 13, 1942.

³⁰ Elder, Robert E. *Information Machine: The United States Information Agency and American Foreign Policy*, pgs. 34-35.

³¹ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 3.

³² Elder, Robert E. *Information Machine: The United States Information Agency and American Foreign Policy*, pg. 36.

³³ IBID, pg. 36-37.

of the United States Information Agency (USIA, known as USIS overseas) on August 1, 1953.³⁴

The USIA inherited two important information campaigns leftover from the end of the war: one in Japan and one in what became West Germany. The goal of the campaigns was to create governance and public cultures in both countries that would be peaceful, democratic, and, as the Cold War started, anchored firmly in the West. These campaigns were eventually deemed, “the most successful single events in postwar U.S. overseas ideological operations.”³⁵ This success, along with the Soviet and Communist challenges, helped build crucial Congressional support for the increased spending required to fund for the first time an ongoing U.S. government commitment to propaganda and ideological warfare (to use two terms common at the time).

From the end of WWII, through the advent of the USIA and up to the collapse of the Soviet Union in the 1990s, “American diplomats and propagandists were no longer reserves to be called up in time of international emergency. They were on the front line of a Cold War”³⁶ and a key factor in U.S. foreign policy.³⁷ As such, the USIA became “Washington’s chosen instrument for ideological operations during the Cold War,”³⁸ an ‘integrated information machine’ closely tied with the government’s other foreign policy elements as part of the country’s overall foreign

³⁴ IBID, pg. 38-39.

³⁵ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 40.

³⁶ Elder, Robert E. *Information Machine: The United States Information Agency and American Foreign Policy*, pg. 45.

³⁷ Armistead, Leigh, *Information Operations Matters*, pg. 71

³⁸ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 4.

policy mechanism.³⁹ At its peak during the Cold War, the USIA had the most extensive presence of any Washington agency; its USIS division operated in almost 300 cities and towns around the world.⁴⁰ “Overall, it was the biggest information and cultural effort ever mounted by one society to influence the attitudes and actions of men and women beyond its borders.”⁴¹ The reader will note the difference with current U.S. information efforts, especially as compared with current Russian efforts.

The USIA worked mainly through the media tools (books, magazines, films, radio, TV) of the time, while also overseeing English language education programs abroad and exchanges between U.S. and foreign academics, artists, scientists, and other professionals. Details include:⁴²

- *Voice of America*, heard by 100 million people during the Cold War years
- Magazines, books, pamphlets, leaflets, and news bulletins printed in over 100 languages, with tens of billions of copies distributed
- A global library network that was the first to introduce open-shelf book access in 150 countries
- The largest English-teaching program ever mounted, including the training of tens of thousands of foreign English teachers
- Exhibits on American life that drew millions of visitors overseas

³⁹ Elder, Robert E. *Information Machine: The United States Information Agency and American Foreign Policy*, pg. 320.

⁴⁰ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 4.

⁴¹ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 4.

⁴² Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pgs. 4-5.

- Exchange programs, including the well-known Fulbright awards (with over 200,000 participants), that brought millions to the U.S. and sent similar numbers of Americans abroad

The data above, while impressive in its commitment to contesting the information environment, contains mainly *measures of performance*: the number of magazines printed, number of visitors at an exhibit, number of people tuned to a broadcast or watching a film in a theater – all items that can be readily counted and measured. Measures of performance are good for determining whether and how often something happened, but are less valuable in measuring the success, failure, or effects of an activity or overall operation.

Beyond measures of performance lie *measures of effectiveness*: the, at times nebulous, concept of whether something actually worked. Did the 10,000 leaflets result in the desired effect in the information environment, or were they largely unread, ignored, or ineffective? Were they, for example, dropped during a rainstorm, turning to unreadable pulp by the time they hit the ground?

In the rainy-day case, the *measure of performance* would indicate a success, for the leaflets were all dropped – the job was done. However, the more important *measure of effectiveness* would indicate failure. No one could read the sodden masses of paper, therefore they created no effect in the information environment, other than perhaps irritation among the populace at having to clean up thousands of pieces of wet paper. In short, if a measure of performance is how many times a class was taught, and for how long, a measure of effectiveness would be how much

students improved on similar tests administered at the start and end of the semester.

In the information environment, measures of effectiveness are notoriously difficult to develop and measure. Did the Warsaw Pact countries overthrow their Communist rulers for economic reasons, because they were tired of waiting in lines for material goods? Or because an information campaign made them aware others had access to better goods without such lines? Or because General Secretary Gorbachev telegraphed he would refrain from unleashing a military response? Or was it a combination of these and other factors?

This lack of clarity compels us to urge caution whenever an information campaign is deemed (in)effective. Accurately measuring opinion is difficult (e.g. the 2016 U.S. presidential election), measuring it from afar without access to the measured populace is an order of magnitude more difficult, attempting to determine which members of that inaccessible populace changed their opinion (and changed it due to a specific action) can be more akin to divinity than science. “What will be forever unmeasurable is the influence of [information-related] activities on foreign perceptions of the United States. The [USIA]’s objectives rested on the most elusive of human acts—changing someone else’s mind.”⁴³

This Research

As briefly highlighted above, information has long been a part of U.S. foreign policy and national security. These efforts have seen successes, failures, and a litany

⁴³ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 5.

of unknowns and inconclusives. The research in this paper attempts to quantify, measure, and compare the effectiveness of information tools, but differs from previous research in two key ways: first, it focuses not on a particular message, but on measures to attenuate censorship; second, it attempts to quantify and compare official, rather than public, reaction to outside events. This focus on measuring official/state opinion rather than public opinion helps avoid the difficulties with populace-focused opinion surveys discussed above.

Heavily influencing our research, compared to previous efforts, is the advent of the internet and related cyber tools. Infiltrating tens of thousands of physical items (from leaflets to magazines and shortwave radios) into a country is a task several orders of magnitude more difficult than taking advantage of existing internet infrastructure, mobile communications technology, and social media to infiltrate similar numbers of cyber messages.

The cyber domain is still developing doctrine, tools, and norms for how states interact with one-another, and with commercial, non-state, and other actors, not just during conflict, but also in terms of diplomacy, espionage, and trade. One emerging norm is the idea that the more open to and reliant a state is on the internet, the more vulnerable it is to cyberattacks. This vulnerability includes the U.S., as highlighted by the intelligence community,⁴⁴ the White House National Security Strategy,⁴⁵ and even the threat assessment of the U.S. Government

⁴⁴ Clapper, James. Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee. Washington, DC, 2016.

⁴⁵ Obama, Barack. "National Security Strategy 2015." The White House, February 2015.

Accountability Office (GAO).⁴⁶ The GAO reporting is important because it is responsible for auditing the security of U.S. government networks – despite years of GAO audits and warnings, a federal database of background check information was hacked by China in 2015, resulting in the theft of the most intimate tax, financial, medical, criminal, address history, and other details of 21.5 million people, essentially every American who has held a security clearance over the past 15 years (including the author of this paper).⁴⁷

For example, though the U.S. military stands as an uncontested superpower in both conventional and nuclear force, “its overwhelming military superiority and its leading edge in information technology have also made the United States the country most vulnerable to cyber-attack. Other nations know that they have fallen behind in military muscle, so they have begun to look to other methods for bolstering their war-fighting and defense capacities [...]”⁴⁸

The EU has also seen what skilled cyber attackers can do to a country reliant on the internet, for example, during attacks on Estonia in 2007 – attacks which even in that less internet-reliant era paralyzed the state and brought governance and the economy “to its knees.”⁴⁹ In Asia, South Korea has seen computer networks “paralyzed in cyberattacks,” damaging systems ranging from air traffic control to those in banking, ATMs, GPS, and major media broadcasters.⁵⁰

⁴⁶ GAO. “Cybersecurity.” U.S. Government Accountability Office (GAO), 2015.

⁴⁷ Davis, Julie Hirschfeld. “Hacking of Government Computers Exposed 21.5 Million People.” *The New York Times*. July 9, 2005.

⁴⁸ Adams, *Virtual Defense*, pg. 1.

⁴⁹ Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Security* 4, no. 2 (2011): 49-60.

⁵⁰ Choe, Sang-hun. “Computer Networks in South Korea Are Paralyzed in Cyberattacks.” *The New York Times*, March 20, 2013.

The examples here, taken from the U.S., Europe, and Asia, help underpin the idea that economically developed, democratic states that rely on the internet are uniquely vulnerable to cyberattacks. A related consensus is emerging that says such states have no effective response mechanism to punish or deter such attacks. In a classic example of a ‘Goldilocks effect’, a military response is viewed as too strong, diplomatic complaints are viewed as too weak, and economic measures are viewed alternatively as too strong, too ineffective, or too slow – leaving nothing viewed as just right. Note, for our purposes, that an information-based response is rarely considered.

Conversely, a related emerging ‘cyber norm’ is that states less reliant on, or capable of exerting more powerful control over, domestic cyberspace and information access are less vulnerable to cyberattacks. Under this idea, termed by one noted researcher the *garrison cyber system*, states “anchored in high sovereign control over cyber venues,” expand current practices of control or denial of access to information to prevent citizens from accessing politically undesirable content.⁵¹ This control helps insulate such states from cyberattacks, while their more open peers remain vulnerable. For example, “The advances in computing and communications and the fundamental shift in strategic affairs associated with the RMA [revolution in military affairs] therefore provide China, at least in Beijing’s eyes, with an opportunity to benefit disproportionately relative to its rivals,”⁵² since

⁵¹ Choucrist, Nazli. *Cyberpolitics in International Relations*, pgs. 234-236. The author credits Harold Lasswell, the creator of the term “garrison state” 60 years ago, for the idea of naming the term/model *garrison cyber system*.

⁵² Newmyer, *The Revolution in Military Affairs with Chinese Characteristics*, pg. 483.

Beijing can exert control over its information environment (and populace) to an extent liberal, democratic states cannot match.

An even more isolated state like North Korea, with essentially zero reliance on the internet for day-to-day commercial, governance, social, or other activities, is seen as even safer from cyberattacks due to this even greater isolation – there is little for an outside cyber actor to attack. The North's competitor to the South, one of the most wired nations on the planet, is dependent on the internet for nearly every facet of modern life, from communications to banking, entertainment to navigation. This dependence creates a rich target set for an outside actor wishing to disrupt, spy on, or influence the South, its businesses, government, and populace – a vulnerability the North has exploited multiple times, with no sign of an effective response or deterrence measure yet devised by Seoul.

This paper does not address the initial point – that states or organizations (from corporations to terrorist groups) are vulnerable to cyberattacks to the extent that they depend on cyberspace to function. A skilled mathematician could likely develop a formula expressing this ratio, this sliding scale of reliance and vulnerability. When such research is released, we greatly look forward to reading it.

What this paper does focus on is the second point, the much less common idea that states tightly controlling of their cyberspace, media, and other information sources (i.e. their domestic information environment) are vulnerable to having that control threatened, challenged or undermined. As discussed at the opening, this paper will determine whether authoritarian states react to the outside use of information as a foreign policy tool to threaten or pressure the regime, including as

compared to more traditional tools of foreign policy. A positive finding here will then assist states, like South Korea, in developing additional response options that allow for an information-based response to an information-based attack, helping reduce or obviate the Goldilocks effect mentioned above.

IR Approaches

Next, the research examines international relations (IR) approaches to see what they say about the use of information as a foreign policy tool. While the paper endeavors to remain agnostic as to approach, an overview of the topic helps situate our research in the broader IR and political science fields.

The first and most important finding is the relative scarcity of related research. “Theory and research on the emergence of the global information society say very little about security, and, when they do, the focus lies primarily on the security of firms and markets rather than the security of states and societies. There is also a specific literature on war and terror in the digital age, which typically comes in the form of idiosyncratic policy analyses, but which does not communicate with the more general theory and research, and is very weak in terms of theoretical application and development.”⁵³

Reardon and Choucri, in *The Role of Cyberspace in International Relations: A View of the Literature*, have conducted perhaps the most detailed survey of journal articles discussing cyberspace and the internet in international relations. Their study looked at major journal articles on cyberspace and international relations

⁵³ Eriksson and Giacomello, *The Information Revolution*, pg. 223.

“from 26 major policy, scholarly IR, and political science journals between the years 2001-2010. This yielded 49 articles, mostly from policy journals. We then looked for common elements across these 49 articles in order to identify the basic contours of the state-of-the-art of the IR and policy communities’ engagement with issues related to cyberspace.”⁵⁴

The survey found three themes common across the 49 articles: the first theme encompassed the problem of defining the cyber domain and related politically relevant phenomena; the second theme addressed the alternately ridiculed and ballyhooed “transformative power of cyberspace;” and the third theme took the analysis several levels higher by attempting to answer, or at least frame, “the question of how international politics and technological change are interrelated.”⁵⁵ The first theme, defining the cyber domain and politically relevant phenomena, “are conceptual puzzles of the first order, and require greater attention from scholars and policy practitioners.”⁵⁶ Our research here does not attempt to advance the field within this first theme. We rely on definitions of the cyber domain and politically relevant phenomena already common in the literature.

The second theme, the grandiose-sounding ‘transformative power of cyberspace’, concentrates “on which actors cyberspace will empower (or in some cases disempower), and what the ultimate effects those changes will be for human freedom and material well-being. In fact, the best of these articles move beyond the

⁵⁴ Reardon and Choucri, *The Role of Cyberspace in International Relations: A View of the Literature*, pg. 28.

⁵⁵ Reardon and Choucri, *The Role of Cyberspace in International Relations: A View of the Literature*, pgs. 25-27.

⁵⁶ Reardon and Choucri, *The Role of Cyberspace in International Relations: A View of the Literature*, pg. 26.

simple – and poorly specified – question of whether cyberspace is eroding the authority of states, and instead look at the ways in which different actors, both state and non-state, may be empowered in different ways and to different degrees under various conditions. However, by situating these questions within narrowly defined issue areas, the authors mostly overlook important ways in which these issues are connected.”⁵⁷

Our research aligns more closely with this second theme. By demonstrating how both state and non-state actors are harnessing cyberspace and the information domain to advance or protect their interests, our research will contribute to this aspect of the field, especially in terms of states that attempt to control information and internet access for domestic constituencies.

The third theme, how international politics and technological change are interrelated, reflects a higher level of analysis and progress made in understanding the dual nature of cyberspace, at once “both technical and material on the one hand, and political on the other. [...] This design is continuously contested by a wide set of international actors. The outcome of this contestation, and in turn, the technical evolution of the Internet, will be determined according to the limits imposed on this system by the physical world, the interests of the various actors, and the political institutions that shape the contest. Similarly, cyberspace itself can impose limits on this political contest, and affect its outcome.”⁵⁸ The key is understanding the duality

⁵⁷ Reardon and Choucri, *The Role of Cyberspace in International Relations: A View of the Literature*, pg. 26.

⁵⁸ Reardon and Choucri, *The Role of Cyberspace in International Relations: A View of the Literature*, pg. 27.

of this nature, rather than viewing technology and cyberspace as a “purely material, apolitical, and exogenous influence on international relations, as is often implicit in the IR literature.”⁵⁹

By attempting to understand how (and how effectively) state or non-state actors use information tools to threaten states that restrict their domestic information environment, our research addresses the third broad theme in terms of how cyberspace can affect the decision-making of targeted states. Specifically, we examine the contestation between states attempting to restrict, by both technical and political means, information flows from cyberspace, and the state and non-state actors attempting to harness those flows to advance their interests. While we attempt to avoid aligning with any of the dominant IR approaches in this paper, our research related to the power and influence of non-state actors lends support to theories that include non-state actors as significant players in international relations.

From this brief survey of IR research, we can see that related research exists, especially within the second theme. However, the related research is either much more specific than ours, addressing, for example, specific technical means to conduct a cyberattack; or the related research is far broader, discussing overall concepts and ontology – for example, *what is a cyberattack, what is cybersecurity*. Our research is unique among that surveyed in both its methodology and in being agnostic as to cyber tool or technique. None of the research surveyed adopts our

⁵⁹ Reardon and Choucri, *The Role of Cyberspace in International Relations: A View of the Literature*, pg. 27.

comparative approach (e.g. between different states, or different tools of foreign policy) or attempts to develop a rubric that measures and analyzes state sentiment as a way of actually testing the effectiveness of cyber/information tools. In short, our research makes a positive contribution to the field through unique methodology, fresh data, and creative approaches to assessment.

Out of all the articles surveyed, including both those examined in the Reardon and Choucri survey, and in our own research, only a November 2010 article from *Foreign Affairs* by Eric Schmidt (Chair and CEO of Google) and Jared Cohen (Council on Foreign Relations and Director of Google Ideas) came close to our work.⁶⁰ Though lacking data and a specific research methodology, many of the arguments made in the article match the topics examined in our research: whether powerful, democratic states may better adjust to the digital era than poorer or more closed states, the idea of “a constant struggle between those striving to promote [...] ‘the freedom to connect’ and those who view that freedom as inimical to their political survival,”⁶¹ and the idea that non-state actors can play a role powerful enough to affect the decision-making of nation states. Despite a general overlap in terms of these broad issues, our research adds data, sentiment analysis of targeted states, comparative measures across a range of foreign policy tools, and a methodology to test and demonstrate our findings.

Aside from the one *Foreign Affairs* article, we have seen very little that closely matches our research approach, methodology, and topics. Even including the

⁶⁰ Schmidt and Cohen, *The Digital Disruption: Connectivity and the Diffusion of Power*.

⁶¹ Schmidt and Cohen, *The Digital Disruption: Connectivity and the Diffusion of Power*, pg. 2.

Foreign Affairs article, none of the articles examined made an attempt to quantify and test the effects of information tools, nor use quantitative measures to test existing theories of international relations. Given that scarcity of related research, why bother with the survey, why even include IR approaches in this paper?

“Even skeptics who doubt cyberspace can play a transformative role in international politics should be eager to subject common claims to critical and rigorous tests. Moreover, given that significant and growing public resources are now being expended to address various aspects of ‘cyberpolitics’, including cyber security and military strategy, and the promotion of international access to cyberspace as a way to encourage global economic development and democratization, one could argue that social scientists have an obligation to address these issues, particularly if they are skeptical of these endeavors.”⁶²

Next, we transition from examining the topics and nature of previous research to a brief look at the main IR approaches. This examination specifically seeks to understand each approach’s view of cyberspace and information as a tool of national security, including the wielding of that tool by both state and non-state actors. Since the earth would likely be torn asunder if a discussion of IR did not begin with realism, in the interests of humanity, we turn first to the field’s original approach.

Cyberspace, as an anarchic, ungoverned domain lacking laws, police, and trust, resides quite comfortably in a realist security framework. This comfort is so

⁶² Reardon and Choucri, *The Role of Cyberspace in International Relations: A View of the Literature*, pgs. 2-3.

high that, "In principle, realists do not see a need to revise their theories for understanding security in the digital age. The state is still seen as the main and sometimes only important actor. Moreover, a narrow (military) definition of security is maintained, thus denying that non-state actors may exercise any degree of (military) power. Realists would presumably tackle the challenge of the information revolution in much the same way as they have tackled previous challenges of transnationalization, complex interdependence, and globalization. These trends are seen as epiphenomena, which may very well affect the policies and domestic structures of states, but which do not undermine the anarchic system of international politics, and thus do not affect the primacy of the state as the supreme political unit."⁶³

What makes cyberspace a domain like no other however, is that within its bounds, states typically lack traditional levels of power and control, often *by design*. "While international relations theory and policy recognize the salience of non-state actors, in no arena are they as dominant as in the cyber domain. These non-state actors are the essential and fundamental system organizers and managers. Recall that it was the most powerful state, the United States that delegated to the private sector the operational management of the Internet. This sovereign decision set the rule of the playing field early on. [...] Most, if not all of the fundamental features (or core functions) for seamless cyber interactions will continue to be controlled and managed by non-state entities."⁶⁴

⁶³ Eriksson and Giacomello, *The Information Revolution*, pg. 229.

⁶⁴ Choucri and Clark, *Integrating Cyberspace and International Relations: The Co-Evolution Dilemma*, pg. 12.

Others argue this control of the internet by non-state entities is overblown, “The globalization literature argues that the lowering of traditional barriers to exchange, the exponential growth of the Internet, and the rise of networked nonstate actors conspire to weaken the state’s role in global governance. The globalization literature is wrong; states are still the primary actors. Furthermore, in focusing on the binary question of state power versus nonstate power, these scholars have glossed over the diversity of relationships that can exist between heterogeneous actors in world politics. A recognition of the substitutability of global governance structures gives us a more powerful lens with which to observe the ramifications of globalization. A review of Internet governance demonstrates that even when states prefer to let private actors take the governance lead, they will intervene to advance their desired ends.”⁶⁵

Liberalism may agree with realism that states play the key role in international relations, but liberals also assign roles, agency, and power to non-state actors. “Thus liberalism has the potential to show awareness of the emergence of new online groups, operating in chat rooms and ‘blogs’, and through new types of audio-visual ICTs [information and communications technologies]. In most liberal readings of contemporary world politics, it is argued that the sovereignty of the nation-state is being permeated and fragmented by the development of transnational relations. Though a single transnational actor is seldom able to challenge the political, military, or economic power of a state, the increasingly complex and globally penetrating web of transnational relations perforates

⁶⁵ Drezner, *The Global Governance of the Internet: Bringing the State Back In*, pgs. 497-498.

sovereign states to the extent that sovereignty is hardly more than a symbol of territorial integrity which, in reality, is no longer sustainable.”⁶⁶

“Paradoxically, however, few liberals seem to have apprehended the challenge of the information revolution. Moreover, those that have are still silent on its implications for security.”⁶⁷ So, while liberals appear more comfortable than realists with the idea of powerful non-state actors, little research has been done to incorporate cyberspace and information tools.

Even liberal approaches (e.g. Nye and Keohane’s complex interdependence theory) that have been updated to address the challenges the information age poses to international relations remain lacking in terms of security. “The costs of interdependence are framed merely in economic terms, and are not portrayed as matters of national or international security.”⁶⁸

Nye’s theory of soft power would appear uniquely salient for our information-focused research. Soft power is “the ability to get what you want through attraction rather than coercion or payments. It arises from the attractiveness of a country’s culture, political ideals, and policies. [...] When you can get others to admire your ideals and to want what you want, you do not have to spend as much on sticks and carrots to move them in your direction.”⁶⁹

Implicit in this argument is that the target audience, the “others” in Nye’s framework, actually have access to your country’s culture, political ideals, and

⁶⁶ Eriksson and Giacomello, *The Information Revolution*, pg. 230.

⁶⁷ Eriksson and Giacomello, *The Information Revolution*, pg. 231.

⁶⁸ Eriksson and Giacomello, *The Information Revolution*, pg. 231.

⁶⁹ Nye, *Soft Power: The Means to Success in World Politics*, pgs. 9, 10.

policies – your attractiveness. Explicit in our research however is that this access is not always possible/available, especially in states that actively seek to censor and control their domestic information environment. Though this effort by states to keep out information that conflicts with government-preferred narratives may in fact be a tacit acknowledgement of soft power's threat, without further research to measure this possibility, the utility of the soft power theory for our purposes is limited. Even if our research manages to develop data or findings supportive of soft power, Nye's focus on economic and military power, with no "attempt to elaborate, critique, or place images of cyber-security threats within his own theoretical framework,"⁷⁰ limits its applicability to our research.

"If idealism and the fear of treading on realist ground by doing security analysis are removed, liberal theory implicitly provides insight into the nature of security in the digital age. In particular, it does so by paying due attention to the increasing plurality and significance of non-state actors."⁷¹ This lack of attention to security leaves room for our research, especially in our similarities with soft power, to further contribute to the field, but leaves us wary that our research may better suit a different IR theory.

Constructivism "most directly addresses the question of whether cyber technology has a transformative effect on the international system by examining its ability to promote the development of new transnational actors that transcend and challenge the authority of states. It is not surprising that constructivists have taken

⁷⁰ Eriksson and Giacomello, *The Information Revolution*, pg. 231.

⁷¹ Eriksson and Giacomello, *The Information Revolution*, pg. 231.

the lead in this area, as constructivism is in many ways best suited to address changes to identity through communicative action, a central mechanism for the development of a global civil society.”⁷²

Like the other approaches however, and despite its apparent suitability to an arena with powerful non-state actors, constructivism has also written little about cyberspace and information tools. What little has been written has mainly emphasized “how information warfare challenges a multitude of boundaries, notably, boundaries of identity.”⁷³ While state concerns over the challenge outside information poses to government-sanctioned narratives and identities may be an important factor in states choosing to tightly regulate their domestic information environment, that is largely outside the scope of this paper. Rather than investigating why states choose to protect their domestic identity through censorship, our focus is trying to determine how states react when that censorship (rather than the identity narrative itself) is challenged. An important and necessary distinction illustrating how our paper largely lies outside previous constructivist research.

Though Marxism is rarely discussed today, it was, ironically, a Marxist sociologist, Manuel Castells, who was among “the first and most influential prophets of the digital age. As early as the late 1980s, he noted that information had become the major primary resource of material productivity in the newly emerging ‘knowledge economy’. It was only a matter of time before information, in the 1990s,

⁷² Reardon and Choucri, *The Role of Cyberspace in International Relations: A View of the Literature*, pg. 8.

⁷³ Eriksson and Giacomello, *The Information Revolution*, pg. 234.

would become an indispensable cornerstone for modern, advanced societies.”⁷⁴

Though of lesser utility in today’s world than when it was written, this Marxist insight from the 1980s remains valid and not out of step with our assertion that information can be used as a tool of foreign policy and national security on par with military, diplomatic, and economic tools.

From our brief survey of the main IR approaches, we have clearly seen a lack of progress assimilating cyberspace, cyber security, and information tools into IR. “Until recently cyberspace was considered largely a matter of *low politics* [italics in original] – the term used to denote background conditions and routine decisions and processes. By contrast *high politics* [italics in original] is about national security, core institutions, and decision systems that are critical to the state, its interests, and its underlying values. We now see cyberspace shaping the domain of high politics, and high politics shaping the future of cyberspace. The field of international relations, rooted in 20th century issues and theories, has not kept pace with the emerging significance of cyberspace.”⁷⁵

From a different set of scholars, disaggregating the topic into policy-oriented and theory-oriented writings. “The specialist literature on security in the digital age is policy oriented with little or no ambition to apply or contribute to theory, and IR scholars have, with few exceptions, paid only scant attention to the security problems of the digital age.”⁷⁶

⁷⁴ Eriksson and Giacomello, *The Information Revolution*, pg. 223.

⁷⁵ Choucri and Clark, *Integrating Cyberspace and International Relations: The Co-Evolution Dilemma*, pg. 2.

⁷⁶ Eriksson and Giacomello, *The Information Revolution*, pg. 235.

From the latter quote, guilty as charged – our paper is also policy oriented with little ambition to apply or contribute to IR theory. Part of the reason for this, for our work and likely that of others, is that none of the dominant IR approaches are a natural fit. Our primarily state-state focus lends itself well to realism, but the idea of cyberspace and information as a tool of foreign policy and national security, including the use of the tool by non-state actors to effectively influence nation states, quickly leaves the realm of realism for the lands of liberalism and constructivism. Breaking across artificial barriers between theories in search of a more applied, realistic model is hardly a crime, and may indeed explain why, roughly two decades on, so little research encompassing security in the digital age has found its way into mainstream IR theories. While it is still too earlier to tell, the research undertaken here may eventually find a comfortable home in one of the approaches. We will revisit this question at the conclusion of the paper.

Communications and Media Studies

The fields of Communications and Media Studies provide theories, models, and effects related to how information can and has served as a tool of foreign policy and national security. Concepts related to our research are outlined below.

Two relatively recent terms repeatedly surface when discussing the media and possible effect(s) on foreign policy. The first of these terms, coined in the early 1990s and including related scholarship, became known as the *CNN effect*. This effect “conceptualised media as a largely domestic-level influence over government decisions for or against intervention into humanitarian crises in regions with

relatively low inherent strategic value, so-called ‘other people’s wars’.”⁷⁷ In essence, the term describes how international mass media (with CNN circa the early 1990s as the archetype) influenced its audience through broadcasting live, 24-hour TV coverage of events that heretofore may have been ignored or escaped the attention of large numbers of the public. This attention had the *effect* of influencing states (chiefly the U.S. in many of the research examples) to become involved in conflicts and humanitarian crises they would otherwise have ignored or avoided. Common examples include the “1991 Kurdish crisis in Northern Iraq, Somalia in 1991–2, Bosnia in 1994–5 and Kosovo in 1999.”⁷⁸ Research suggests that the coverage of the event led the public (*viewers* of the news, rather than *readers* of the news) to influence government(s) to take action(s) they might otherwise not have considered – in short, a media/information effect on foreign policy. This effect and related research however, soon faded in favor of a broader term that goes beyond satellite TV to include cyberspace.

That newer, somewhat more nuanced term, emerged in the 2000s and was branded, *the Al Jazeera effect*:

“Al Jazeera is a paradigm of new media’s influence. Ten years ago, there was much talk about ‘the CNN effect’, the theory that news coverage—especially gripping visual storytelling—was influencing foreign policy throughout the world. Today, ‘the Al Jazeera effect’ takes that a significant step farther. The concept encompasses the use of new media as tools in every aspect

⁷⁷ Gilboa et al., *Moving Media and Conflict Studies Beyond the CNN Effect*, pg. 3.

⁷⁸ Gilboa et al., *Moving Media and Conflict Studies Beyond the CNN Effect*, pg. 3.

*of global affairs [...] traditional ways of shaping global politics have been superseded by the influence of new media—satellite television, the Internet, and other high-tech tools. What is involved is more than a refinement of established practices. We are seeing a comprehensive reconnecting of the global village and reshaping of how the world works.”*⁷⁹

While *CNN effect* refers to the power of live, 24/7 international news media, *Al Jazeera effect* broadens to include the internet, social media, mobile communications and other ‘new media’ tools. Equally as important, *Al Jazeera effect* also includes the idea of regionally-based, regionally-focused, culturally-relevant content delivered in the language (e.g. Arabic) of the intended audience, unlike Western-based international media like CNN, which function primarily in English and can be perceived as having a Western cultural and political bias.

These two ‘effects’ are salient to the research here, not in terms of their narrative or content, but in their examples of how public access to previously unavailable information can affect government policies and the related concerns this can create for governments, especially those unaccustomed to outside information competing with official government narratives. These new information sources, “have added to a ground swell of public opinion that Arab governments have found they cannot ignore. From the Atlantic to the Indian Ocean, Arab

⁷⁹ Seib, *The Al Jazeera Effect: How the New Global Media Are Reshaping World Politics*, pg. preface.

governments are worried they have lost control of information, one of the key means they have used to stay in power in the past.”⁸⁰

The quote above, about Arab government concerns over the loss of information control, was written in 2000 – a decade before the events that came to be known as ‘The Arab Spring’, uprisings commonly blamed/credited at least partially to that loss of information control. Taken together, these two effects, especially the broader, more culturally-attuned *Al Jazeera effect*, are applicable to our research in that they describe what *could* happen should publics suddenly gain access to new, powerful, enticing, language-appropriate media content. As these effects appear to demonstrate, this access can become a threat for governments not used to competing against outside, unapproved narratives. One early issue however, is that these effects lack models, or associated, prescriptive, falsifiable theories. While this detracts from our ability to harness them for this paper, it does provide a clear area for future research.

Aside from these two, relatively recent, effects, lie more traditional theories of communications. The seminal early work for communications theory and modeling, the Shannon-Weaver Model, defines communication as “all of the procedures by which one mind may affect another,”⁸¹ and breaks down the process into three levels: technical (how accurate can the communication be transmitted), semantic (how precisely does the communication convey the desired meaning), and effectiveness (does the received meaning affect conduct in the desired way).⁸² Since

⁸⁰ Henderson, “The ‘al-Jazeera Effect’: Arab Satellite Television and Public Opinion.”

⁸¹ Shannon and Weaver, *The Mathematical Theory of Communication*, pg. 3.

⁸² Shannon and Weaver, *The Mathematical Theory of Communication*, pg. 4.

our research is agnostic as to message, the technical level is the main one with applicability here – our focus is access to information outside of government-approved channels, not the content or meaning of the message, nor whether that meaning created a desired effect.

The 1949 Shannon-Weaver model contributed to 1960's Sender-Message-Channel-Receiver (SMCR) communication model. Each of these four main components contain multiple factors (e.g. the attitudes, knowledge, and cultures of the sender and receiver, the method by which the message was sent and delivered, etc.).⁸³ This later model is criticized for lacking a feedback (or two-way communication) mechanism and its assumption of no 'noise' or other barriers in the communication process. This model's assumption of no barriers in the communication process creates obvious complications in attempting to use it for the research purposes here, as does its focus on attitudes, knowledge, and cultures – all important factors in communication, but outside the research scope of this paper, where the focus remains on the ability to access outside information, presumably of meaning to the person attempting to access the information.

Together, these two models, and later evolutions, have become known as the *message influence model* and have remained influential well into the post 9/11 world, including as part of the messaging recommendations from the 9/11 Commission.⁸⁴ Recent critics however, have blamed the message influence model

⁸³ Berlo, David. *The Process of Communication: An Introduction to Theory and Practice*.

⁸⁴ Corman, Trethewey, and Goodall, *A 21st Century Model for Communication in the Global War of Ideas*, pgs. 4 and 6.

for failing to “deliver success.”⁸⁵ Aside from the problems outlined above as part of our research (e.g. the assumption of no or only limited barriers to message delivery), critics highlight two additional key problems: 1) failures to understand local context, culture, languages, and power relations – the social structure and milieu of the targeted message recipient(s) and 2) an overemphasis on message (e.g. a focus on crafting the “magic bullet” message that will convince the recipient) rather than developing a more comprehensive messaging strategy designed to disrupt existing belief systems enough to provoke the formation of new “meaning-making frameworks” that can allow for achieving the effect(s) desired by the message sender.⁸⁶

Newer theories take a more systems-based approach that focuses on “the *process* surrounding the communication of messages [italics in original]”⁸⁷ and the overall complexity of the systems in which the sender and receiver exist and communicate. Interestingly for our purposes here, one of the key principles of this newer model is ‘disruptive moves’ that can upset the structure of the existing system.⁸⁸ These disruptions are thought to be possible ‘game changers’ that can break through existing ‘noise’ in the system and allow for reconstituted belief systems that include ideas desired by the message sender.⁸⁹ In terms of our

⁸⁵ Corman, Trethewey, and Goodall, *A 21st Century Model for Communication in the Global War of Ideas*, pgs. 7-9.

⁸⁶ Corman, Trethewey, and Goodall, *A 21st Century Model for Communication in the Global War of Ideas*, pgs. 7-9.

⁸⁷ Corman, Trethewey, and Goodall, *A 21st Century Model for Communication in the Global War of Ideas*, pg. 9.

⁸⁸ Corman, Trethewey, and Goodall, *A 21st Century Model for Communication in the Global War of Ideas*, pgs. 13-14.

⁸⁹ Corman, Trethewey, and Goodall, *A 21st Century Model for Communication in the Global War of Ideas*, pgs. 13-14.

research, sudden access by a population to outside information, unofficial narratives, and open domestic communication free of government control may count as one of these game-changing disruptions, or create enough concern in the leadership of the targeted state to allow the threat of a disruption to be used as a foreign policy tool. Aside from this possibly useful principle, our research's agnosticism as to message largely obviates any remaining connections to the principles in both the old and new communications models discussed here.

The communications theories examined above largely reflect the dominant, 'mainstream' ideas of the field. However, there is a less common model that may have a connection to our research and bears examination, the *Propaganda Model* of Edward Herman and Noam Chomsky. In the words of the authors, "the propaganda model describes forces that shape what the media does; it does not imply that any propaganda emanating from the media is always effective. [...] The public is not sovereign over the media—the owners and managers, seeking ads, decide what is to be offered, and the public must choose among these."⁹⁰

The quote above is from the updated *Introduction* to the 2002 edition of the original 1988 work that launched the theory. The new introduction focuses on updating the model to include changes to the media landscape engendered by the internet. The authors found that new, online media did not substantially alter the findings of the model, "In short, the changes in politics and communication over the past dozen years have tended on balance to enhance the applicability of the

⁹⁰ Herman and Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media*, pg. Introduction.

propaganda model. The increase in corporate power and global reach, the mergers and further centralization of the media, and the decline of public broadcasting, have made bottom-line considerations more influential both in the United States and abroad.”⁹¹

We can see from the quotes above, describing both the original 1980s model and 2002 update, that the focus of the model, per the title of the book (*Manufacturing Consent: The Political Economy of the Mass Media*), is on political economy – the power and financial structures of major media corporations and the effects this has on their choice of content and messaging. Further, per the authors, “As we have stressed throughout this book, the U.S. media do not function in the manner of the propaganda system of a totalitarian state.”⁹² While a valuable, landmark model, it primarily examines how the (mass) media serve as defenders of a status quo that favors certain privileged groups – well outside the authoritarian-state, information-access focus of our research.

In sum, of the media and communications effects, theories, and models examined here, we see two points salient to this research:

1. The Al Jazeera effect, for its examination of how authoritarian states (primarily in the Arabic-speaking world) view threats to their control of information and an official narrative.

⁹¹ Herman and Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media*, pg. Introduction.

⁹² Herman and Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media*, pg. Conclusions.

2. The idea of 'disruptive moves' that upset the structure of existing systems, allowing for 'game changers' that break through existing system noise/stasis, allowing for reconstituted belief systems possibly of use to the 'disruptor' – a key point to remember here is leadership in a targeted state/organization believing that a (potential or operationalized) move could be disruptive.

While these two ideas provide insights for our research, like the IR theories examined above, neither represent a model or theory around which to organize this paper. This again highlights both the applied nature of our work and the need for a new framework that better explains the role of information and information access as a tool of foreign policy and national security.

History and Background

Whether controlled by state or non-state entities, is information as a tool of conflict and international relations even all that new? Surely cyberspace has increased the speed and size of the network, but information as a tool of war, "has been a central element in military thinking at least since Chinese strategist Sun Tzu wrote his famous *The Art of War* some 2000 years ago. Electronic warfare, such as the electronic jamming of radio communication, has been an element of interstate conflict for a much shorter time (since the Second World War), but is also a precursor of the much more recent talk of warfare in the digital age. The introduction of information warfare in strategic studies and military planning

(which generally has been informed by realist thinking) could be seen as a marker of continuity rather than dramatic change. Some of the technology is new, as is the global capacity of resourceful digital adversaries, but the basic notions of attacking and defending information and information systems are as old as warfare itself – basically, old wine in new bottles.”⁹³

Similarly, authoritarian governments and others wishing to control the information that reaches their constituencies have long gone to great lengths to censor, restrict, and monitor information flows. In an effort to control the underground ‘samizdat’ press (censored materials reproduced and distributed by hand), for example, the former Soviet Union restricted access to copy machines.⁹⁴ This was in addition to jamming radio and TV frequencies used by outside broadcasters like the BBC and Voice of America.

For decades, Sovietologists attempted to study the effects of these information flows, including the aforementioned samizdat press, on the Soviet Union and associated authoritarian regimes in Eastern Europe and Central Asia. As discussed at the start of this chapter, the U.S. Information Agency (USIA/USIS), was in many ways built around the idea that broadcasting, publishing, and infiltrating outside information into closed societies would benefit U.S. foreign policy.⁹⁵ ⁹⁶ The agency (1953-1999) attempted to study the effects of its information operations to see whether, for example, it had any justification in claiming to have helped usher in

⁹³ Eriksson and Giacomello, *The Information Revolution*, pg. 229.

⁹⁴ For more on Soviet history and regulation of photocopiers and the samizdat press, please see Soldatov, Andrei, and Irina Borogan. *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*. 2015, pgs. 3-23.

⁹⁵ U.S. Information Agency, archived 1999 website.

⁹⁶ U.S. National Archives, Records of the U.S. Information Agency (RG 306).

the collapse of the Communist Bloc or end apartheid in South Africa. We will briefly examine three of these studies.

First, in Eastern Europe, some, including members of Poland's Solidarity movement, credit information dissemination for helping end Communist control, initially in Eastern Europe, then in the Soviet Union.⁹⁷ For example, after the collapse of the Soviet Bloc in Eastern Europe, a Solidarity-led coalition came to power in Poland (Solidarity was an anti-Soviet, anti-Communism trade union movement in Poland from the late 1970s). Of the first group of 22 cabinet ministers, 11 of them, including the prime minister, were alumni of USIA exchanges, as were 44 members of the new parliament.⁹⁸

Second, in apartheid South Africa, the USIA's exchange programs are credited with aiding the struggle to end apartheid. Frederick de Klerk, the last president of the white-dominated era, "was instrumental in modifying hardline apartheid policies. Among other actions, he released Nelson Mandela from his long prison sentence. De Klerk later acknowledged that his [USIA-funded] study visit to the United States strongly influenced his views on civil rights in South Africa."⁹⁹

Third, and perhaps most interesting, the USIA played a key role during the coup in the Soviet Union in August 1991 that ended the rule of Mikhail Gorbachev and led to the rule of Boris Yeltsin and dissolution of the Soviet Union. During the coup, hardline elements opposed to Gorbachev seized control of the nation's radio and television stations, but not international phone/fax lines or broadcast jammers.

⁹⁷ Taylor, Philip M. "Munitions of the Mind". Third Edition. pg. 285

⁹⁸ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 204.

⁹⁹ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 207.

The Voice of America's Moscow correspondent was able to report on the crisis by phone from inside the city, and the VOA was able to broadcast unjammed news updates into Russia every 10 minutes around the clock during the crisis. More importantly, Gorbachev's foreign minister was able to get out a fax requesting the USIA use its transmitters to broadcast a message from Boris Yeltsin to the Soviet Army, bypassing the coup leaders. "The effectiveness of Voice of America broadcasts was later acknowledged in a statement to VOA officials from the All-Russian State Television and Broadcasting Co.: 'Millions of Soviet people, denied the possibility of receiving information from Russian sources, listened to your Voice. It inspired them with faith and determination to fight dictatorship.'"¹⁰⁰ This official thank-you letter from the Soviet Union's state broadcaster to the VOA for the broadcasts supporting the fight against dictatorship provides a rare but valuable measure of effectiveness. It is hard to imagine Russia's current state media sending a similar letter.

These three brief examples highlight an era when the U.S. government (along with the governments of most major world powers) funded and tasked an organization specifically designed to implement information as a tool of foreign policy. The examples above, lacking quantifiable data and hardly conclusive, still serve to highlight the possibilities of information tools in the pre-cyber age.

More recently, during the Arab Spring of 2011, authoritarian countries throughout the Middle East and North Africa were quick to tighten information controls on traditional media, cyberspace, and social media in an effort to control

¹⁰⁰ This section is largely from Dizard, Wilson, *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pgs. 210-211.

news of the mass uprisings and (perhaps more importantly) prevent people from communicating privately to plan demonstrations and other activities seen as endangering the state. In January 2011, the Egyptian government first blocked whole websites, including Facebook and Twitter, before finally shutting down mobile service and the country's access to the Internet entirely in late January.^{101 102} Outside the region, China and North Korea simply banned and censored all mention of 'Arab Spring' and related terms from their domestic information environments.

It is helpful to pause here to note the combination of government and private sector organizations highlighted above. While the USIA/USIS was a government entity attempting to affect change in targeted states, Facebook and Twitter are most certainly not – they are neither government entities nor seeking to advance a government narrative. In short, they are commercial non-state entities affecting the decision-making of nation states. The advent of the internet has further developed the idea that commercial firms, from Hollywood to the advertising industry, have “emerged as the largest force[s] influencing America's ideological impact abroad.”¹⁰³ “If the United States government had tried to come up with a scheme to spread its brand of capitalism and its emphasis on political liberalism around the world, it couldn't have invented a better model than the Internet.”¹⁰⁴

The goal of this brief history lesson has been to highlight that information has long been a part of international relations and provides abundant examples of

¹⁰¹ Dunn, “Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising.”

¹⁰² Cornell University Library, The January 25 Revolution.

¹⁰³ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 5.

¹⁰⁴ Lohr, Steve. “Ideas & Trends: Net Americana; Welcome to the Internet, The First Global Colony.” *The New York Times*. January 9, 2000.

possible successes. However, the difficulty lies in moving beyond correlation that the information operations *may* have caused the outcome into demonstrating the information operations *caused* the outcome. The research examples provided above contain solid qualitative findings, but lack quantitative measures that could lend additional support to claims of effectiveness.

Our research differs from previous research in three key ways: first, it adds a quantitative measure capable not only of demonstrating the reactions caused by the information operation, but also allowing for a comparative measure with other tools of foreign policy and national security. Second, our research does not focus on a particular message or narrative – we are not, for example, attempting to measure the effectiveness of a narrative attempting to undermine apartheid or communism. Instead, our focus is on access to information, specifically, access to information not owned or controlled by the state – we are agnostic as to the content of the non-state-controlled information flows. Third, much of the existing research, including that highlighted in the examples above, focuses on public reaction rather than official reaction. Attempts to undermine communism and apartheid, and related attempts to measure the effectiveness of the campaigns, focused on changes in public opinion. Our research is the opposite – we focus on *state* reaction to information operations, specifically the threat or actual operationalization of an information campaign that would undermine/limit/degrade the effectiveness of the targeted state's information controls.

Compared to the historical examples highlighted above, our research provides three unique additions to the field of information as a tool of international

relations. Whether one believes information tools are age-old wine in new bottles or legitimately new capabilities brought on by cyberspace and the internet age is largely irrelevant to our research; we are simply attempting to creatively use new research methodologies to better measure the tool's (in)effectiveness.

DIME

Information has long been viewed as part of national power under the *DIME* construct, which divides the instruments of national power into four elements: diplomatic, information, military, and economic.¹⁰⁵ In the U.S., the Department of State takes the lead on diplomacy, the Department of Defense on military, and the Departments of Commerce and the Treasury have the lead on the economic instruments of statecraft.

However, since the demise of the USIA in 1999, no one organization in the U.S. has had the lead on the information element, despite some experts calling for a new organization to do exactly that.¹⁰⁶ The State Department, including the remnants of the USIA, has taken the lead on strategic-level information operations, while the DoD and elements of the intelligence community (e.g. the CIA) have taken the lead at the operational and tactical levels, and in areas often associated with espionage.

Ironically, just as the internet and cyberspace began to grow in importance, the U.S. government disbanded the USIA, the one organization focused on efforts in

¹⁰⁵ U.S. Department of Defense, "Joint Publication 1: Doctrine for the Armed Forces of the United States," pgs. I-11 to I-14.

¹⁰⁶ Nagl, John A., "Knife Fights: A Memoir of Modern War in Theory and Practice", pgs. 135-136.

the information environment. All that remains is a pledge that the various instruments of national power will make “every effort to synchronize, align, and coordinate communication activities.”¹⁰⁷

This incongruity is highlighted by John Nagl, influential scholar on counterinsurgency and counterterrorism theory, and co-author of the U.S. military’s counterinsurgency manual. “During the Cold War, the U.S. Information Agency (USIA) conducted effective information operations against the Soviet Union, although that war was primarily economic, secondly military, and only thirdly an information war. USIA was closed at the end of the Cold War as a budget savings measure. The war against radical Islamic extremism, on the other hand, is *primarily* [italics in original] a war of ideas, but we have no organization in charge of fighting that part of the fight. The national failure to rebuild the U.S. Information Agency, which did such good work during the Cold War but was a casualty of the peace dividend, has cost lives and treasure over a decade of war that would have been far better fought with someone in charge of information operations.”¹⁰⁸

Aside from the DIME construct, *political warfare* is a concept at least as old as Sun Tzu and found advocates in the U.S. during the Cold War (e.g. George Kennan¹⁰⁹), as well as more recent proponents.^{110 111} The concept is a broad one, and includes (per Kennan), “all the means at a nation’s command, short of war, to

¹⁰⁷ U.S. Department of Defense, “Joint Publication 1: Doctrine for the Armed Forces of the United States,” pg. I-12.

¹⁰⁸ Nagl, John A., “Knife Fights: A Memoir of Modern War in Theory and Practice”, pgs. 135-136.

¹⁰⁹ Kennan, George. “The Inauguration of Organized Political Warfare.” U.S. Department of State.

¹¹⁰ Boot, Max, and Michael Doran. “Political Warfare: Policy Innovation Memorandum.” Council on Foreign Relations.

¹¹¹ Robinson et al. “Modern Political Warfare: Current Practices and Possible Responses.” RAND Corporation.

achieve its national objectives.” However, per RAND, “The term political warfare is not ideal for a variety of reasons,”¹¹² not least of which is the broadness of the concept. As an aggregation of all means short of war, disaggregation of the various tools of statecraft for research and comparative purposes is problematic and therefore the concept was not selected as the framework for this paper.

While political warfare may be overly broad or nebulous, an alternate construct, PMESII-PT, used by the U.S. Army (and some other organizations, many conducting Army-funded studies) is the opposite – overly narrow and restrictive. The acronym stands for Political, Military, Economic, Social, Infrastructure, Information, Physical Environment, and Time and appears more useful at the operational and tactical levels of military and intelligence operations than the strategic level statecraft tools examined here.

Finally, an expanded version of DIME exists, DIMEFIL. The latter adds financial, intelligence, and law enforcement elements to the original four DIME tools. Perhaps useful for specific operational and tactical level approaches, the expanded version of the concept contains little of benefit for the research here. In addition, like PMESII-PT, it is rarely used outside of U.S. Army and related works, limiting its portability for non-military audiences compared to DIME.

While the other concepts outlined here may be useful at certain levels and for certain activities (e.g. intelligence, law enforcement), for the reasons discussed above the DIME construct provides the clearest, broadest research framework for

¹¹² Robinson et al. “Modern Political Warfare: Current Practices and Possible Responses.” RAND Corporation.

this paper. In addition, the framework's familiarity to both academics and practitioners increases the portability of our research and any policy recommendations across both of these domains. For these reasons, our research chapters are built around the DIME framework.

Russia

One of the earliest advocates of information campaigns as a political tool, specifically radio broadcasting, was Vladimir Lenin, who saw them as a way to consolidate Communist authority across the Soviet Union.¹¹³ Prior to his death in 1924, he ordered a "massive expansion of Soviet domestic radio broadcasting to allow Communist authorities in Moscow" to better assert control over the new nation's far-flung empire.¹¹⁴

While the tools may have changed, Russia remains a world leader in cyber and information operations. In Russia's latest national security strategy, from December 2015, the elements of power are divided into a far broader variety of subcomponents than that of its Chinese or American counterparts: "national defense; state and social security; quality of life of Russian citizens; economic growth; science, technology, and education; health; culture; and ecology and environment."¹¹⁵ Though much of this laundry list appears outside the foreign policy and national security realms, the national security strategy's emphasis on domestic economic development and improving the quality of life for Russians is at

¹¹³ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 23.

¹¹⁴ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 23.

¹¹⁵ Olikier, "Unpacking Russia's New National Security Strategy."

least partly attributable to the age-old Russian bugaboo that threats from within are at least as important as threats from without.¹¹⁶

The specific threats include: NATO expansion, 'Color Revolutions' by those working from within and without to undermine Russia's territorial integrity and destabilize its political processes, and not least, information warfare.¹¹⁷ The information warfare aspect of Russia's strategy is of particular saliency here, with outside observers stating that Russia has come to see the emerging "global 'information space'" as exploitable terrain capable of altering the global balance of power, with no issue "more important or more fraught with uncertainty than the current and future information environment."¹¹⁸

Highlighted by a 2013 article from the Chief of the General Staff of the Russian Federation, General Valery Gerasimov, warfare in the 21st century is defined by new, 'non-linear' rules. "The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. [...] The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures. All this is supplemented by military means of a concealed character, including carrying out actions of information conflict [...]."¹¹⁹

¹¹⁶ Olikier, "Unpacking Russia's New National Security Strategy."

¹¹⁷ Klimentyev, Michael. "Russia's National Security Strategy for 2016 in 9 Key Points."

¹¹⁸ Tatham, pg. 54.

¹¹⁹ Gerasimov, Valery. "The Value of Science in Prediction." *Military-Industrial Kurier*, February 27, 2013.

Russia is viewed as a world leader in this new style of ‘hybrid’ or ‘non-linear’ warfare, the concept of which “gained new momentum after the Russian operations in Crimea and Eastern Ukraine in 2014 that seemed to follow a script very much in line with General Valery Gerasimov’s 2013 doctrine of ‘non-linear war’.”¹²⁰ The U.S. election in November 2016 also included allegations of interference by a Russian information operation campaign. We will further examine Russian activities in the information environment, including the importance of the ‘hybrid warfare’ doctrine, in the chapter on Russia.

The contrast between the U.S. approach, where the information element of national power is arguably the least important of the four elements, and the centrality of information to the Chinese and Russian approaches, demonstrates not only differing views of the importance of power and control of the information environment, but also the asymmetrical approaches common among states facing a conventionally superior competitor.

North Korea

Unlike Russia and the U.S., North Korea has published little on its national security strategy or military doctrine. This makes the North perhaps the world’s most problematic country in terms of understanding its national security strategy and military doctrine. Here the research turns to outside specialists – diplomats, Korean Studies scholars, and international security specialists, many of whom have

¹²⁰ Svetoka, Sanda, and Anna Reynolds. *Social Media as a Tool of Hybrid Warfare*, 2016, pg. 9.

reached a general consensus that information is an underutilized tool for managing relations with the North. Decades of diplomatic, economic, and military tools targeting Pyongyang have failed to achieve international goals backed by the U.S., South Korea, Japan, the EU, and other members of the international community. With that failure, or at least, with the currently underperforming level of stasis, many Korea specialists have theorized or outright advocated for harnessing the flow of information, cyber and otherwise, to reduce North Korean threats to regional stability and human rights.

To date however, though Korean Studies texts (from both scholars and foreign policy practitioners) are rife with descriptions of information tools as an important but underutilized resource for influencing the North Korean regime, many of the recommendations are untested and anecdotal, with little qualitative or quantitative supporting data – areas of concern we attempt to address in this paper.

As mentioned above, research from the early Cold War onwards has examined the threat posed to authoritarian (mainly communist) states by the flow of outside, unregulated information entering their controlled domestic information environments.¹²¹ ¹²² Much of this research has been theoretical, or based largely on interviews¹²³ and anecdotal reporting,¹²⁴ with little data (especially quantitative data) developed to support or challenge the idea that unregulated information flows

¹²¹ Snyder, Alvin. *Warriors of Disinformation: American Propaganda, Soviet Lies, and the Winning of the Cold War, An Insider's Account*. 1st ed. New York: Arcade Publishing, 1997.

¹²² Elder, Robert E. *Information Machine: The United States Information Agency and American Foreign Policy*. 1st ed. Syracuse University Press, 1968.

¹²³ Armistead, Leigh. *Information Operations Matters*. 1st ed. Washington, DC: Potomac Books, Inc., 2010, pgs. 20-21.

¹²⁴ Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*. Boulder and London: Lynne Rienner Publishers, 2004.

are (or are at least viewed by leadership as) a threat to the state. This lack of data has also limited research into how threats in the information environment compare to threats in the diplomatic, economic, and military realms – returning us to our central research question as to whether information tools can be used as effectively in achieving foreign policy goals as diplomatic, economic, and military tools.

Digital Humanities

Fortunately, developments in the relatively new field of digital humanities may provide an opportunity to address the research and data gap mentioned above. Thanks to this new field, researchers now have access to data mining and text analysis tools largely unheard of a generation, or even a decade, ago. These new tools assist our research by allowing us to find, analyze, and compare national government reactions to outside stimuli, including reactions to information, economic, diplomatic, and military threats.

Combining the more established event databases and tools from political science (e.g. *The Correlates of War Project*, <http://www.correlatesofwar.org/> or START's *Global Terrorism Database*, <https://www.start.umd.edu/>) with newer tools and media analysis (e.g. *The GDELT Project*, <http://www.gdeltproject.org> or *Media Cloud*, <http://mediacloud.org>), many researchers have harnessed digital humanities tools to analyze *popular* reaction to political, financial, and international events. Results gleaned from this data have already been successfully commercialized (e.g. *Geofeedia*: <https://geofeedia.com/>, *Dataminr*: <http://dataminr.com/>, *Scraawl*:

<https://www.scraawl.com>) and demonstrated their usefulness to journalists, security specialists, and firms in the financial industry.

Comparatively fewer researchers have used the tools to analyze *official government* reaction to events. By aggregating and analyzing reactions to events published in official state media, we gain a tool for measuring and comparing government responses to outside stimuli in the diplomatic, information, military, and economic categories. For this analysis to be successful, it requires a model for quantifying, categorizing, and ranking what begins life as qualitative, text-based data. Essentially, we need to convert the text of official state media reports and government pronouncements reacting to outside events in the DIME realms into quantifiable data. The research methodology chapter, below, illustrates how we will use the tools described here, in the DIME categories and building on previous IR research, to create and exploit such a model.

Conclusion

Our research incorporates and builds on existing work from multiple fields: political science and international relations, public policy, area studies, history, and digital humanities. The overall approach is grounded in political science and international relations, but benefits from (and makes additional contributions to) area studies, history, and public policy by adding data and tools from digital humanities. By combining these elements, we answer the question of how information tools can affect the strategic calculus of states with closed or tightly restricted information environments. Our research, even a negative finding that

information has no or negligible effect on state decisions, benefits each of these fields in turn. We now turn to a more specific description of our research methodology.

Chapter Three: Research Methodology

As outlined in the previous chapter, the countries initially selected for our research are Russia and North Korea. Pyongyang is widely viewed as the most restrictive country in the world in terms of its domestic information environment. Russia, though less restrictive than North Korea, is still viewed as restrictive, and was selected due to concerns any findings on North Korea may be skewed due to the relatively unique level of control Pyongyang exerts over its information environment – Russia essentially provides balance and the possibility of broadening the scope of any findings.

The countries were also selected due to their importance in the realms of foreign policy and national security. The determination of the relative freedom of their domestic information environments is informed by previous research from *Reporters Without Borders* (<http://en.rsf.org>) and *Freedom House* (<https://freedomhouse.org>). Both of these independent, non-governmental organizations publish widely respected data and related rankings, broken down by country, on the freedoms of information, the press, and access to the internet.

Our research was primarily conducted in English, with the exception of GDELT data (more on GDELT below). GDELT ingests data from dozens of languages, categorizes it into events, and conducts sentiment analysis; anyone researching with GDELT can avail themselves of this translation capability. This provides access to, for example, Russian language media sources, greatly extending the scope of our data, with the caveat that GDELT relies on machine-based translation, event

categorization, and sentiment analysis. More on these caveats and related tradeoffs below.

Aside from GDELT data, the research focuses on reports from state-owned or controlled media outlets, including related Twitter accounts. For Russia, the research also includes related statements from the foreign ministry website, an option unavailable for North Korea.

Media Sources

The media sources for each country are listed below. Further details and background on the sources are available in the separate country chapters. When available, the sources' related Twitter account will also be examined.

- North Korea: the official *Korean Central News Agency* (KCNA – <http://www.kcna.kp>), the *The Rodong Sinmun* (the newspaper of the ruling Workers'/Labor Party – <http://www.rodong.rep.kp>), and *Uriminzokkiri* (<http://www.uriminzokkiri.com/>).
- Russia: the government-owned TASS news agency (<http://tass.ru>), also referred to as *ITAR-TASS*, and the foreign ministry's website (<http://www.mid.ru/>), containing hundreds of official documents, press releases, regime commentary, and interviews with the foreign minister and other key officials.

Key Events

Below, broken down by country and then by DIME, are examples of events for our initial research. The full, comprehensive list of events is found in each country's chapter.

Example events (and DIME category) for Korea include the December 2015 UN vote to condemn North Korea's human rights (diplomatic), the March 2016 imposition of UN sanctions and the December 2011 imposition of EU sanctions (economic), the March 2016 ("largest ever") U.S. and South Korean Key Resolve/Foal Eagle military exercises (military), and the August 2015 loudspeaker broadcasts by South Korea into North Korea (information).

Example events (and DIME category) for Russia include the 27 March 2014 UN General Assembly response to Russia's invasion of Crimea (diplomatic), the 6 March 2014 U.S. decision to impose sanctions on Russia for violation of Ukrainian sovereignty and territorial integrity (economic), the five-week long NATO Trident Juncture exercise starting 19 October 2015 (military), and the annual reports from *Reporters without Borders* and *Freedom House* calling for governments around the world to allow greater press freedom and access to the internet (information). These are just examples; additional events will be developed for each category in the respective research chapters.

Once an event is selected, we will search for reports referencing it on the websites of the state media outlet(s) and foreign ministry (when available). All reports referencing the event will be downloaded into an Excel database (some events generate hundreds of rows of data) containing the title, date, URL, and text of

the reports. The reports are broken down and stored by paragraph to allow for more granular research – this provides the option of determining the article’s overall sentiment, or only the sentiment for the paragraphs focused on the specific event under investigation. Initially, all sentiment analysis will be performed at the document level.

Finding and downloading the event-related reports can be a lengthy, time-consuming process – some events generate dozens of reports, each of which must be found before the appropriate data can be downloaded into the appropriate sections of a database. Finding, copying, and pasting all of the related reports into a spreadsheet can take weeks per event, and is ripe for operator error during the hours of drudgery.

Fortunately, there are automated tools that can be programmed to handle this process. For our purposes, we chose the relatively affordable Parsehub (<https://www.parsehub.com/>). The web-based application, once given a URL, can be quickly programmed to navigate a website and retrieve specific portions of specific pages. For example, given the URL of a search results page on the Russian Foreign Ministry website, Parsehub can navigate to each of the search results, grab the title, date, URL, and text, then download that information into a spreadsheet formatted by the title, date, URL, and text.

For example, if we are looking to examine Moscow’s reaction to U.S. economic sanctions enacted on March 13, 2014, we can have Parsehub retrieve all stories with related search terms (e.g. *US* and *economic sanctions*) between 15 February 2014 and 15 April 2014 from the websites being examined. This provides

us with dozens, hundreds, and occasionally thousands of rows of spreadsheet data representing reporting on the event, sectioned into columns for title, URL, date, and the actual text of the story. Once this event data has been collected, we can begin our analysis.

Event Analysis and Digital Humanities

Once the reports are successfully downloaded and stored in Excel (per above, a lengthy, resource-intensive process – even once automated), they are ready for analysis of sentiment, dates, and number(s). The number of reports is a proxy for the ‘importance’ of an event – the more reports, the more attention the event received (or provoked). By overlapping dates with the number of reports, we can track how events garner attention over time.

Next, by disaggregating the events into the four DIME categories, we can track and compare how different types of events generate reporting over time. By adding sentiment analysis of the text of the reports, we can measure and track sentiment over time and by event, again broken down into the DIME categories. Sentiment analysis is key – it allows us to see whether an event is generating positive, negative, or neutral sentiment, and the ratio thereof, which in turn allows for a comparison of how positively or negatively a government responds to specific outside event stimuli.

Together, these measurements allow us to track and compare how governments react to the words (e.g. threats, demands) and actions (economic sanctions, military maneuvers) taken by outside governments and organizations

(e.g. NGOs, the UN) over time. This is key to addressing our research question of whether authoritarian states react to information as a tool of foreign policy and how those reactions (if any) compare to reactions to diplomatic, economic, and military tools.

These questions are answered in the research chapters on Russia and North Korea. First however, are some brief details on two key components of the research: digital humanities and sentiment analysis. The first is, broadly, an emerging field and family of research tools, the latter is a key member of that family of tools and one this research will use extensively.

As briefly discussed in the literature review chapter, the field of digital humanities (DH) sits at the intersection of humanities and computer science, allowing students and researchers to analyze datasets in minutes or hours that would take years (or a lifetime) using traditional methods. By using these tools, scholars can, for example, quickly examine and quantify years of newspaper reporting in dozens of languages to model state-state interaction, discover new patterns in the works of Shakespeare by examining his entire corpus, or search the 450+ volumes of documents from the U.S. State Department's Foreign Relations of the United States (FRUS) series – mining for specific words, testing concepts, and creating new models along the way. DH may come to stand alone as a new discipline, like computer science; or it may remain not a species, but a genus – no more than a random collection of apps.¹²⁵ Whichever it becomes, the tools and

¹²⁵ Kirsch, *Technology Is Taking Over English Departments: The False Promise of the Digital Humanities*, May 2, 2014.

capabilities it brings are useful to scholars in all fields, including the two disciplines closest to our work here: political science and area studies.

Of those digital humanities tools, the one most crucial to our research is *sentiment analysis*, defined by two leaders in the field as, “the computational treatment of opinion, sentiment, and subjectivity in text.”¹²⁶ In a sense, turning text, from whatever the source, into quantifiable data, or, as others have succinctly described it, “sentiment analysis is opinion turned into code.”¹²⁷

By analyzing the sentiment of a report, or even better, tens of thousands of reports, researchers can quantify opinion on a topic. For example, by performing sentiment analysis on all Russian Foreign Ministry website documents pertaining to NATO military exercises in Eastern Europe, researchers gain a proxy for Russian government reaction to events of a military nature. Repeating this process for other events (e.g. UN resolutions, economic sanctions), and for other countries, allows for the quantifiable measurement and comparison of government reactions to events in the categories of diplomacy, information, military, and economics.

It is important to note that, at this stage, sentiment analysis in English is far more developed than in other languages.¹²⁸ Developing a language-specific corpus with appropriate sentiment coding and related tools is the ideal way of performing sentiment analysis; other methods (including machine translating the content into English, then performing the analysis) are available, but viewed as less

¹²⁶ Pang and Lee, *Opinion Mining and Sentiment Analysis*, 2008, pg. 6.

¹²⁷ Mia, *Editor's Choice: Sentiment Analysis Is Opinion Turned into Code*, April 7, 2015.

¹²⁸ Korayem, Khalifeh, and Crandall, *Sentiment/Subjectivity Analysis Survey for Languages Other than English*, pgs. 2 and 24.

capable/accurate.¹²⁹ For this paper, we will conduct sentiment analysis of English content from each country examined, in addition to sentiment analysis of machine translated material for non-English content (using GDEL, described below).

To perform and display sentiment analysis, this research uses two programs: *MeaningCloud* and *Tableau*. MeaningCloud (<https://www.meaningcloud.com/>) is an easy-to-use tool which can be installed and integrated into Excel. Once set up and functioning in a spreadsheet of data, the user selects the cells with the text to be analyzed, then initiates the sentiment analysis process. MeaningCloud is integrated with Excel but does all of its analysis remotely – meaning each cell of text is uploaded to MeaningCloud’s servers (which ensures the user is accessing the most recent version of the program and corpus and provides the ‘cloud’ portion of the name). Once uploaded, the text is analyzed, then returned and added to a new sheet in Excel. The new sheet contains the original text, a few additional details, and the sentiment analysis itself, expressed as a range from P+ (very positive), to P (positive), NEU (neutral), NONE (none – no sentiment), N (negative), and N+ (very negative).

MeaningCloud (or any sentiment analysis system) determines what is positive, neutral, etc. by examining/determining the polarity of the different sentences in the text and the relationship between the sentences, which results in a global polarity value for the whole text (e.g. sentence, paragraph, group of paragraphs, document), followed by natural language processing techniques to also

¹²⁹ Korayem, Khalifeh, and Crandall, *Sentiment/Subjectivity Analysis Survey for Languages Other than English*, pg. 24.

detect the polarity associated with entities and concepts in the text.¹³⁰ Together, this provides the sentiment value that determines whether the text is classified as very positive (P+), positive (P), neutral (N), etc.

For example, the following sentence from the Russian Ministry of Foreign Affairs (MOFA) website was categorized as *very negative* (N+), “A series of terrorist attacks rocked Jakarta at about 11 am on January 14, perpetrated by suicide bombers and gunmen in the centre and other parts of the Indonesian capital. Preliminary reports suggest seven people died, including police. There has been no information of victims among Russian citizens.” In comparison, the following MOFA example was categorized as *negative* (N), “In its allegations against Russia, the French Foreign Ministry relies on someone’s speculations and propaganda clichés rather than on specific facts.” Comparing the “terrorist attacks,” “suicide bombers,” and deaths described in the previous, very negative example, with the “allegations,” “speculations,” etc. from the negative example helps illustrate the difference in sentiment.

An example of *neutral* (NEU) text, also from MOFA’s website, “The work to find practical solutions to the Ukrainian crisis will continue at the next Contact Group meeting scheduled for January 20.” From the example, the sentiment contains both broadly positive (“practical solutions”) and negative (“crisis”) terms, resulting in an overall neutral categorization. Finally, also from MOFA, “The agreement to exchange POWs once again will also help to increase mutual confidence and de-escalate the situation.” This example is categorized as *positive* (P) by MeaningCloud,

¹³⁰ MeaningCloud. “What Is Sentiment Analysis?” MeaningCloud LLC, 2018.

based on “agreement,” “exchange POWs,” “increase mutual confidence,” and “deescalate the situation.” These examples illustrate the capabilities of sentiment analysis, in this case the software behind MeaningCloud, to analyze English-language text to determine sentiment. While other systems, of varying capabilities, exist, most work relatively similar to the examples highlighted here.

Once the MeaningCloud sentiment analysis is complete, the researcher is left with rows and rows of data in an Excel spreadsheet, each row with a paragraph of text and associated sentiment. This presents the problem of how to tabulate, measure, and display the data. Simply adding how many P, P+, N, NEU, etc. measurements are contained for each event is one method, and it can be performed inside Excel, but it only provides the totals, without incorporating the number of sources or dates. More importantly, this method does not allow the researcher to track the sentiment and number of sources (the number of sources is a proxy for the importance of the story) over time. To track and display all of this information, a more powerful data visualization tool is needed.

For data visualizations, this research used Tableau (<http://tableau.com/>), not only the leader in the field, but a company kind enough to offer fully-capable, free versions of its software to students. After importing the spreadsheet into Tableau, users can create timelines, charts, etc. that highlight the specific data they are trying to analyze. The example below, built from GDELT data, illustrates Russian government sentiment toward the U.S. government from June 2012 to September 2016. We will explain the timeline in greater detail after the image.

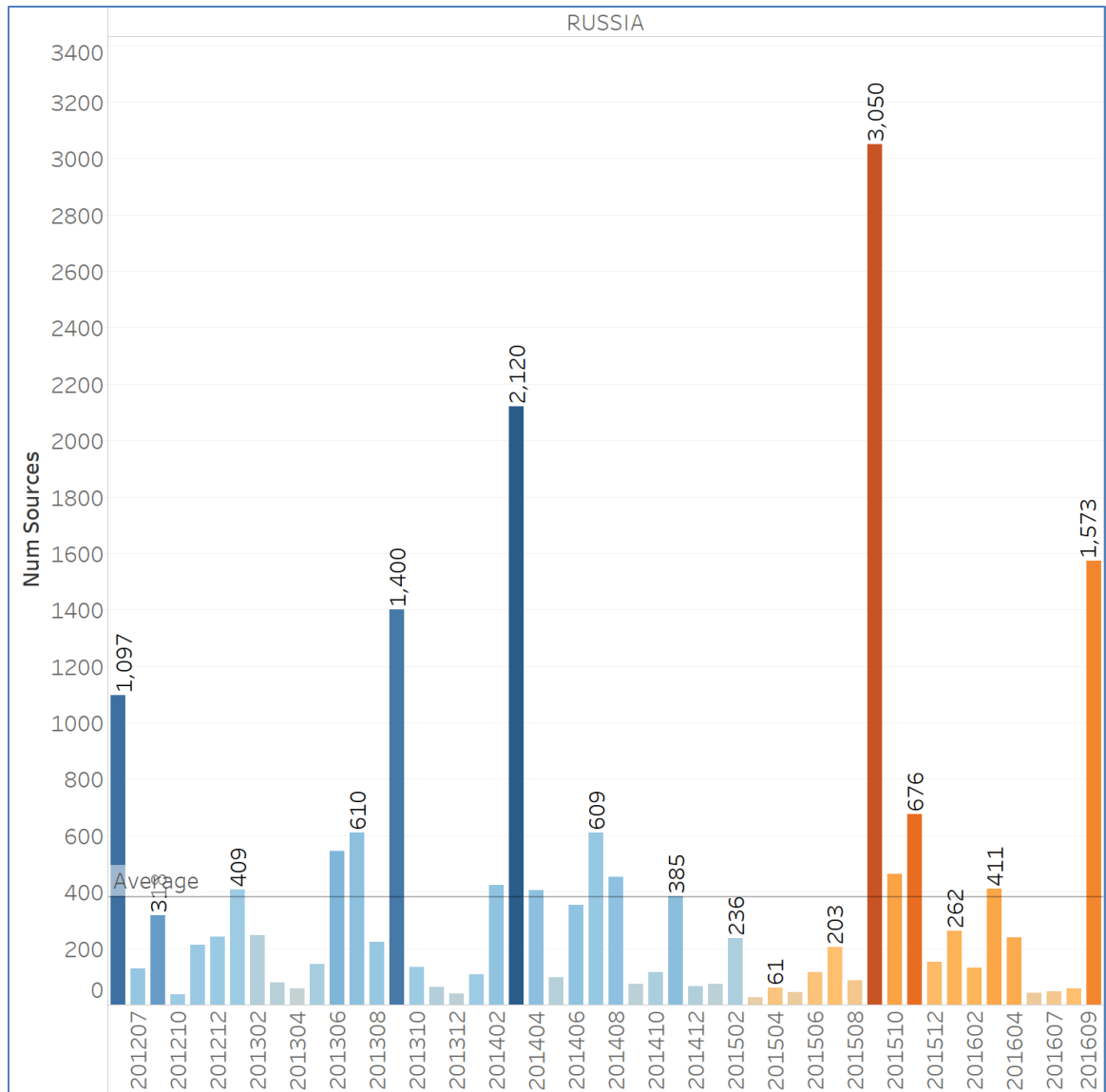


Figure 3: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016.

The dates of the timeline are at the bottom; the number of sources is along the left (one source = one mention of one event by one article). The colors represent sentiment: the darker the blue, the more positive; grey is neutral; the redder the orange, the more negative. The numbers at the top of the bars indicate the exact number of sources for that bar in that month. The average line toward the lower

section of the timeline indicates the average number of monthly sources over the time period examined.

From the chart, we can quickly see the greatest number of reports by Russian media sources on the U.S. government occurred in March 2014 and September 2015. The March 2014 reporting was quite positive, while the September 2015 reporting was quite negative (and overall reporting turned from positive to negative in early 2015). We will analyze the fuller meaning of this data and chart in the Russia chapter; the goal here is simply to provide an example of how research data is presented in this paper.

By using a tool like Tableau, researchers can combine large amounts of data into a single graphic, allowing for easier-to-read, more efficient presentations. An additional benefit of a tool like Tableau is the ability to produce interactive charts. Though unable to embed the interactive charts into a document like this paper, they can be uploaded and hosted on a related website, offering those reading the paper the ability to explore the data and test both the writer's findings and their own ideas. This tool will be used in addition to, rather than in lieu of, the data and analysis presented here in the paper.

Finally, once this lengthy process of data collection, compilation, categorization, sentiment analysis, and visualization is complete for each event and from each media or government source, we will have findings that demonstrate official government reaction (positive, neutral, and negative), over time, to outside events, all broken down into the four DIME categories. These datasets will be created for each of the countries under examination in this paper.

From these datasets, we can make the analysis and comparisons that define the paper – discovering which category of events at which times affect which governments in which ways. Or, which categories produced no effects, or only faint effects. It is important to note here that finding a category created no effect is still salient. By demonstrating, for example, that economic measures failed to create an effect (or the desired effect) in the target government, policymakers can realize the need to alter or scrap existing plans in favor of a tool with a greater likelihood of success.

GDELT

This research supplements data gained from specific media and event searches with data from GDELT. The brief mention of GDELT above promised additional details, and to that we now turn.

The *GDELT Project* (<http://www.gdeltproject.org>) bills itself as “the largest, most comprehensive, and highest resolution open database of human society ever created. [...] A platform that monitors the world's news media from nearly every corner of every country in print, broadcast, and web formats, in over 100 languages, every moment of every day and that stretches back to January 1, 1979.”¹³¹

The purpose of monitoring news media, and new efforts to monitor social media, is so the GDELT Project can compile (and offer researchers) a database of world events and interactions. The project's database is currently built around 300 categories of “physical activities” around the world. These activities, or “events,” are

¹³¹ GDELT Project website, <http://www.gdeltproject.org>, accessed 7 February 2016.

detailed with nearly 60 data points that help define each event's actors, actions, timelines, and locations.

Unlike similar databases, GDELT makes an extensive effort to go outside the English-speaking world, operating, per above, in over 100 languages and providing what the Project believes "is the largest realtime streaming news machine translation deployment in the world."¹³² GDELT's multilingual database provides researchers with access to event reporting and sentiment analysis from media sources and languages otherwise unavailable, greatly extending the reach of our research.

GDELT is the system for finding and storing the event data, the classification ("coding") of the events is based on the CAMEO (Conflict and Mediation Event Observations) coding system currently developed at Penn State University. CAMEO is, "specifically designed to code events relevant to the mediation of violent conflict but can also be used for studying other types of international interactions."¹³³

As we will see in the research chapters, this focus by GDELT's chosen ontology on events relative to the mediation of violent conflict means the system is far more robust in terms of the diplomacy and military categories of DIME than it is for the economy and information categories. For economy, there are handful of event categories (e.g. *impose sanctions, threaten sanctions, ease economic sanctions*), but overall this category is much less robust than the military and diplomacy categories. The information category is even less developed, with essentially zero

¹³² IBID, accessed 7 February 2016.

¹³³ "GDELT CAMEO: Conflict and Mediation Event Observations; Event and Actor Codebook", Pennsylvania State University, March 2012, pg. 1.

specific information-related event categories, though with several related to laws, human rights, and ‘non-force threats’ that provide some tangential, overlapping coverage.

This imbalance in categories and event coverage reduces the efficacy of GDELT in our research and forces us, for the information category especially, to rely more heavily on the national media and government (e.g. foreign ministry) reporting discussed above. One caveat to this limitation is that it applies to, for example, U.S. government efforts to influence the Russian government in the information category – the system will have trouble capturing the U.S. government’s use of information as a foreign policy tool. However, it would still capture *overall* Russian government sentiment toward the U.S. government. Meaning, the use of GDELT data to develop a timeline measurement of overall Russian government sentiment toward the U.S. government (like in the image above), then using that measurement to gauge Russian government sentiment during *known* information (or economy) category events, would remain an effective use of GDELT. We will readdress this issue and caveat in each of the four country-focused chapters.

Separately, GDELT data displayed on a timeline can also be used to check for sudden ‘spikes’ in the number of sources in a given month. Any spikes that do not correspond to one of our predetermined events could indicate an important event missed in our previous research. This will serve as a check on our initial assessment of key events and a method for detecting ‘new’ events appropriate for further research.

Overall, GDELT brings data, resources, and much-needed linguistic capabilities to our research, though it also brings significant caveats. We note these issues not only here, but in the country-focused research chapters to follow.

Additional Tools for Data Collection and Analysis

Aside from GDELT and the other tools noted above, what other comparable event databases and tools are available? Are there any that could benefit our research? We explore these questions next.

The National Consortium for the Study of Terrorism and Responses to Terrorism, commonly known as START, maintains the “Global Terrorism Database (GTD), an open-source database including information on more than 113,000 domestic and international terrorist events around the world since 1970.”¹³⁴ The database contains event coded information on terrorist incidents, perpetrators, victims, weapons, and attack types, but the focus is on kinetic actions. There is no information on events purely in the information or cyber environments. While this well-known database is commonly used in political science, security studies, and other fields related to our research, the focus on terrorists rather than state-level actors, and the emphasis on events in physical space rather than in the information environment, reduces its utility for the research here.

GDELT, specifically the CAMEO coding system on which it’s built, is related to two older, similar event databases: the World Event/Interaction Survey (WEIS –

¹³⁴ START website, About START, University of Maryland, <https://www.start.umd.edu/about/about-start>, 27 February 2016.

<http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/5211>) and the Conflict and Peace Data Bank (COPDAB – <http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/7767>). “Both were created during the Cold War and assumed a ‘Westphalian-Clausewitzian’ political world in which sovereign states reacted to each other primarily through official diplomacy and military threats. While innovative when first created, these coding systems are not optimal for dealing with contemporary issues [...]”¹³⁵ While CAMEO has faults, as noted above when it comes to the economic and informational tools of foreign policy, it still covers a far wider range of events than these two databases, hence its selection as the primary event database for this paper.

The (somewhat dated) *Lydia* system at Stony Brook University, part of the State University of New York (SUNY) system (<http://www3.cs.stonybrook.edu/~skiena/lydia/>), supports sentiment analysis and web mining (searching cyberspace for specific words and phrases). Lydia has been used to show the frequency of mentions of a topic, business, political leader, sports figure, stock, etc. or to highlight “trends and entity relationships through large-scale analysis of [English-language] blogs.”¹³⁶

Using data from Lydia, researchers can generate a sentiment analysis to determine the percentage of views on a subject that are positive, neutral, or negative. Examples of previous and ongoing projects include stock market

¹³⁵ GDELT CAMEO: Conflict and Mediation Event Observations; Event and Actor Codebook”, Pennsylvania State University, March 2012, pg. 1.

¹³⁶ Lydia/TextMap Publications, Stony Brook University website, <http://www3.cs.stonybrook.edu/~skiena/lydia/>, accessed 7 February 2016.

predictions and the likelihood a movie will succeed, based on sentiment analysis of popular opinion on the topic mined from media and blog-based datasets.

To date, the Lydia system does not appear to have been applied to the foreign policy realm – difficulties with machine-based language translation may have played a role in this, limiting the system’s capabilities outside of the English language information environment and thereby limiting its utility for our research. In addition, the user interface is somewhat dated, lacking the far more advanced search capabilities of the other systems discussed. For these reasons, the Lydia system is not used in this paper.

Media Cloud (<http://mediacloud.org>), a joint project of the Berkman Center for Internet & Society at Harvard University and the Center for Civic Media at MIT, “is an open source, open data platform that allows researchers to answer complex quantitative and qualitative questions about the content of online media.”¹³⁷ The focus of Media Cloud is less about traditional media like newspapers; its focus is online media and how these media cover events and use languages and sources – in some ways more of a tool for examining the media than a tool for using the media to examine events.

Despite its emphasis on examining the media, Media Cloud does offer an interesting tool for our research here, the *Media Cloud Attention Plotter*, “an online tool for graphing and comparing volumes of content from multiple media sources and word frequencies within that content over a range of dates.”¹³⁸ This tool could

¹³⁷ Media Cloud website, <http://mediacloud.org/about/>, 7 February 2016.

¹³⁸ Media Cloud website, <http://mediacloud.org/2014/05/10/attention-plotter-2/>, 7 February 2016.

be used, for example, to determine the number of “comments” versus “denunciations” made by official North Korean media. A look at the sources used by Media Cloud however, turns up no sources from North Korea, but nearly 400 for China, just over 670 for the Russian Federation, and 162 for Iran.¹³⁹ The functionality to compare word frequencies within certain fixed dates (i.e. around foreign policy events of the type under investigation here) while useful, is less capable than GDELT, plus lacks data on North Korea. In addition, Media Cloud’s focus on online media instead of the broader media environment limits this tool’s utility.

Other tools and databases similar to the ones highlighted above exist (e.g. *Opinion Crawl*, <http://www.opinioncrawl.com>), but the ones highlighted represent the leaders in the field. There are also private companies creating similar databases and tools (e.g. *Dataminr*, <http://dataminr.com>), but access to their systems for (non-paying) researchers is unavailable, the scale of their datasets is limited (e.g. *Dataminr* is built almost solely around Twitter), and the focus appears to be on sheer speed. For example, the companies focus on data mining social media to quickly unearth breaking events of interest to journalists, public safety specialists, and the financial industry. While interesting and useful capabilities, they lack the length of time required for our research – for legal, financial, and technical reasons,

¹³⁹ Media Center website (<https://sources.mediameter.org>), Berkman Center for Internet & Society at Harvard University and the Center for Civic Media at MIT, <https://sources.mediameter.org/#media-tag/8876997/details> (China), <https://sources.mediameter.org/#media-tag/8876995/details> (Russia), <https://sources.mediameter.org/#media-tag/8876998/details> (Iran), accessed 6 February 2016.

the companies typically only store data going back several months, whereas we require years of related data.

To date, many of these tools, chiefly the ones focused on social media, have been used primarily to gauge popular opinion, often with an emphasis on speed in order to gain an advantage in predictive analysis (the usefulness of such an advantage in the stock market is clear), or to provide early warning and notification of breaking events. Dataminr has proven especially adept at *quickly* unearthing breaking events (e.g. terrorist attacks) from Twitter's mass of tweets, becoming a trusted resource for police officers and journalists around the world.

While these capabilities are impressive, this research is not about discovering popular opinion; it is about trying to gauge official, *government* opinion. Specifically, government opinion in authoritarian states as a way of measuring the effects of the four foreign policy tools discussed above.

Conclusion

With a unique research need and methodology identified, this paper proposes to conduct research salient to the fields of area studies, political science, public policy, and digital humanities. The results will provide value to both scholars and practitioners, either by identifying an additional tool for use in influencing authoritarian regimes, or by demonstrating that information tools are not the equal of those from diplomacy, economics, and the military.

Any findings that demonstrate the utility of information tools to pressure states as (or more) effectively than traditional foreign policy tools will have

implications for scholars and practitioners in multiple fields. For example, if states react to the threat or operationalization of information tools, what value does this hold for theories of deterrence? A current hot topic in political science is whether and how deterrence can be achieved in cyberspace. Our findings here, given that cyberspace is commonly defined as a subset of the overall information environment, may play a role in this discussion.

Second, outside of the states with restricted domestic information environments under investigation here, any positive findings may have implications in counterterrorism and counterinsurgency. For example, by applying the tools and methodology here to gauge the reaction of key leaders of terrorist and insurgent groups to information flows, we can better judge the effectiveness of pressuring these groups through challenges to an information monopoly or control of a dominant narrative. As reflected in media and social media, including in the official accounts of the organizations and individuals involved, challenges to these groups in the information environment can be tracked, measured, and refined to craft policies that more effectively target and exploit the concerns of terrorists and insurgents.

For example, per discussions in the U.S., does labeling ISIS/Daesh as a major threat actually support the group by building its credibility and thereby aiding recruiting? Or is it better to refer to them in less respectful terms as criminals or incompetents in order to diminish the group's credibility as a method for possibly impairing recruiting? Using the tools and methodology outlined here to gauge the reaction of key ISIS figures to these alternate policies could help determine which is actually viewed as more threatening by the group's leadership, thus helping craft

policies more likely to affect the decision-making calculus of terrorist and insurgent groups.

Based on the literature reviewed above and the research proposed here, this paper has identified and will address an unmet research need. While it builds on research and tools used by predecessors, its proposed contribution will be unique, hold value, and advance academic knowledge in multiple fields.

Chapter Four: Russia

“In the 1950s, the first Soviet photocopy machine had been wrecked because it threatened to spread information beyond the control of those who ruled. Now the power of those rulers was being smashed—by a network they could not control.”¹⁴⁰

This chapter examines Russian government sentiment and actions in response to four different foreign policy tools: diplomatic policy, information policy (which is so rare the term even sounds odd), military policy, and economic policy. By the end, the reader will have a clearer idea of which tools produce the strongest negative reactions in the Russian government, in addition to three nominally unrelated, yet nonetheless interesting findings. The chapter closes with policy recommendations and several suggested areas for future research.

The research into Russia used three broad sources:

1. Official reports, statements, and documents in English from the Russian Foreign Ministry’s website.¹⁴¹
2. English-language stories from the government-owned TASS news agency (<http://tass.ru>), also referred to as ITAR-TASS.¹⁴²

¹⁴⁰ Soldatov, Andrei, and Irina Borogan. *The Red Web: The Struggle between Russia’s Digital Dictators and the New Online Revolutionaries*, 2015, pg. 42.

¹⁴¹ The Ministry of Foreign Affairs of the Russian Federation, http://www.mid.ru/en/main_en, accessed 29 January 2017.

¹⁴² TASS, Russian News Agency, <http://tass.com/>, accessed 29 January 2017.

3. Russian, English, and other language reporting from *GDEL*T, the previously mentioned, “largest, most comprehensive, and highest resolution open database of human society ever created.”¹⁴³

The first two, as noted, rely on English language reports only. *GDEL*T, through its automated translation system, *GDEL*T *Translingual*,¹⁴⁴ offers the ability to use machine-translated Russian (and 64 other) language sources. We note that human translated, or human-verified translations, are generally considered more accurate than machine translations. We also note the ability of machine translation systems to process far more data, tens of thousands of Russian language data points in this case, far more quickly and efficiently than human translators. To quote *GDEL*T, an admittedly biased source, their system grants access to “the entire universe of all possible translations of each sentence to find the translation that will yield the highest quality.”¹⁴⁵ With these caveats in mind, multilingual *GDEL*T data is included in this research.

The Russian government is measured as described previously, across diplomatic, economic, military, and informational categories. Within each category, several events were selected to gauge Russian government reaction through Ministry of Foreign Affairs (MOFA) and state-owned media (TASS) reporting.

¹⁴³ *GDEL*T Project, *The GDEL*T Story, About *GDEL*T, <http://gdeltproject.org/about.html>, accessed 29 November 2016.

¹⁴⁴ *GDEL*T Project, *GDEL*T *Translingual*, <http://blog.gdeltproject.org/gdelt-translingual-translating-the-planet/>, accessed 29 November 2016.

¹⁴⁵ *GDEL*T Project, *GDEL*T *Translingual*, <http://blog.gdeltproject.org/gdelt-translingual-translating-the-planet/>, accessed 29 November 2016.

After MOFA and TASS, the research takes a broader view by using GDELT data from 1 January 2005 to 30 September 2016. Rather than pre-selected events, GDELT allows researchers to examine every interaction between the Russian and U.S. governments (on a monthly basis) across the entire time period, looking for spikes in reporting or changes in sentiment. These spikes or sentiment changes may indicate the governments reacting to outside events, or (and more importantly for this paper), they may indicate governments reacting to outside foreign policy tools. Since the goal in the chapter is to measure the effectiveness of foreign policy tools targeting the Russian government, we are specifically looking for reporting spikes or sentiment changes that reflect Russian government reaction to U.S. government use of any of the four categories of foreign policy tools. The GDELT data allows for the comparison of a range of interactions, for example, Russian government reaction to U.S. government comments, whether positive or negative (*verbal cooperation* or *verbal conflict* in GDELT's ontology) or Russian reaction to very specific U.S. actions, for example, threatening economic sanctions or making an official diplomatic complaint.

Data Collection

The data from TASS was downloaded between August and November 2016, and saved in Excel spreadsheets, one spreadsheet per event. This resulted in spreadsheets totaling over 9,000 rows (and 7 columns) of data, for a total of approximately 63,000 possible data points. The text of the reports was then analyzed for positive/neutral/negative sentiment by the data and sentiment

analysis tool *MeaningCloud*, before being imported into the data analysis and display software, *Tableau*, used to generate the timelines and charts below.

Data from the Ministry of Foreign Affairs (MOFA) was collected between August and November 2016, and then processed in the same manner as the TASS data, as outlined above. The MOFA reports resulted in spreadsheets totaling approximately 41,000 rows (and 7 columns) of data, for a total of approximately 287,000 possible data points.

The GDELT data, covering all U.S. government – Russian government interaction from 1 January 2005 to 30 September 2016, was also downloaded between August and November 2016. Data was downloaded for both the U.S. government and Russian government across the four broadest taxonomic classes allowed by the GDELT database (*verbal cooperation*, *material cooperation*, *verbal conflict*, and *material conflict*). This represents all possible interactions under the GDELT ontology. The data was then combined into a single spreadsheet of 24,318 rows (and 59 columns – totaling over 1.4 million possible data points) covering all U.S. and Russian government interaction during the time period discussed. GDELT includes its own sentiment analysis capability, which was used here in place of *MeaningCloud*, before the data was output to *Tableau* to generate the analysis and charts below.

We examine the data in two different sections: first MOFA and TASS, then GDELT. Within each section, we will examine the data based on our four categories (diplomacy, information, military, and economics). Each of the sections, and then the entire chapter, concludes with a discussion of our findings.

SECTION 1: TASS and MOFA

We start by examining the data from TASS and the Ministry of Foreign Affairs (MOFA). One caveat, MOFA has a practice of posting, verbatim, long transcripts of interviews with the foreign minister. These interviews, occasionally just press releases, address many topics of the day of interest to the Ministry or Foreign Minister. This dilutes the value of that particular article by immersing it within a large body of unrelated commentary. In future, more Russia-focused research, we can attempt to control for this by removing the unrelated passages.

Below are the selected events:

- Diplomatic:
 - the July 2014 UN Security Council resolution condemning the downing of Malaysia Airlines flight 17,
 - the March 2014 UN General Assembly resolution reaffirming the territorial integrity of Ukraine,
 - the April 2010 New START Treaty signed by Presidents Obama and Medvedev.
- Economic:
 - December 2015 U.S. sanctions on Russia over Ukraine,
 - March 2014 EU sanctions in response to Russia's invasion of Crimea/Ukraine,
 - the March 2014 U.S. sanctions on Russia for violation of Ukrainian sovereignty.
- Military:

- the five-week long NATO Trident Juncture exercise starting 19 October 2015, the largest NATO exercise in a decade;
- the Baltic states joining NATO in March 2004;
- the August 2008 NATO dispatch of naval vessels to the Black Sea in response to the Russia-Georgia war;
- U.S. plans for European missile defense (in February 2007 the U.S. started negotiations with Poland and the Czech Republic and in April 2007 Russia announced countermeasures).
- Information:
 - annual reports from *Reporters without Borders* and *Freedom House* on Russia's press freedom and citizens' freedom to access to the internet,
 - the annual release of the U.S. State Department's report on human rights.

Each of these events was ranked in two ways: the number of times the event was referenced by the targeted source (i.e. the number of articles referencing the event on the MOFA and TASS websites) and the sentiment of the text used in the reporting. The greater the number of references to the event, the greater the assessed impact of the event. This serves as a proxy for the 'importance' of an event – more important events generate a larger amount of reporting.

The sentiment of the reporting on the event was then ranked on a five-level scale: N+ (very negative), N (negative), NEU (neutral – neither positive nor

negative), P (positive), and P+ (very positive). For the research here, the negative ratings are more important than the positive ratings. For example, with the number of reports held constant, a diplomatic threat that generated more negative sentiment than an economic threat means the target state, in this case Russia, viewed the diplomatic threat as more dangerous/powerful/threatening than the economic threat. So, for our purposes, the diplomatic tool would be judged more effective than the economic tool at pressuring the target state. Future research could flip this focus, to see which tool is viewed as more rewarding, but the research in this paper focuses on sticks over carrots.

Overview

Of the 16 events selected (some of the bullets above represent multiple events), only two had negative sentiment outweigh positive sentiment: TASS coverage of the July 2014 downing of the Malaysian Airlines flight over the Ukraine (68% negative, 24% positive) and TASS reporting from 2013-2016 on Freedom House (54% negative, 33% positive). All other events, including every event surveyed at the Ministry of Foreign Affairs (MOFA), had positive sentiment outweighing negative sentiment.

Overall, TASS stories were more negative than MOFA stories, with all five of the top five most negative, least positive stories belonging to TASS. The more negative tone of TASS reporting, compared to MOFA reporting, could be due to the diplomatic nature of MOFA, a reflection of TASS' editorial slant, or a combination of

these and other reasons – providing a possible area for future Russia-focused research.

Negative Sentiment

The TASS reporting on the Malaysia Airlines flight, originally categorized under the diplomacy category due to UN Security Council resolution 2166 condemning the crash and calling for an investigation, appears to be an outlier. Russia didn't exercise its Security Council veto power to prevent the resolution and much of the TASS coverage focuses on the crash and loss of life instead of the UN resolution. Though reporting on the crash and loss of life created the most negative sentiment, *mentions of the UN resolution were neutral or slightly positive*, with a clear focus on the need for a fair and impartial investigation. So, while this event received the most negative coverage of any examined here, that negativity is assessed as due to the nature of the event, a downed plane and loss of life, rather than diplomatic pressure. The mixed finding reduces the applicability of this event for our research, but the research methodology successfully identifying the reasons for the negative sentiment (and correctly labeling it negative) underscores the accuracy of our methodology and software tools.

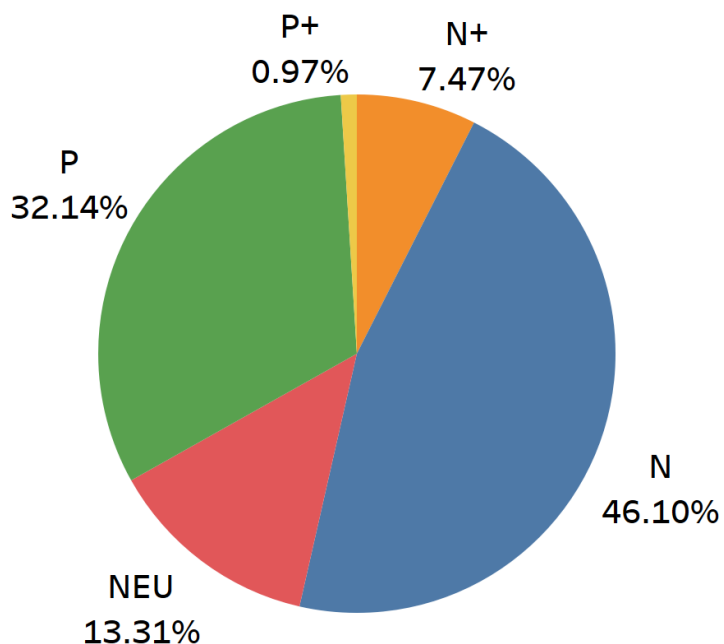
The next event, and the only other one with negative sentiment that outweighs positive sentiment, is more interesting in terms of our research. It comes from the information category, specifically TASS reporting on Freedom House. Freedom House, as a reminder, issues annual reports examining *Freedom on the Net*,

Freedom in the World, Freedom of the Press, and related issues.¹⁴⁶ These reports regularly raise the ire of authoritarian regimes around the world. Russia, while the least restrictive of the four countries examined here, is still regularly placed in the least free category, though with occasional exceptions that place the country in the middle of three categories (*free, partly free, not free*) in terms of freedom on the internet.

Per the image below, over 53% of TASS writings on Freedom House are negative (46%) or very negative (7.5%), compared to 32% positive or only 1% very positive. Per the second image, the relative ratio of negative to positive appears to hold from 2013-2016, the only period since 2008 for which we could find TASS reporting on Freedom House.

Unlike the negative reporting above, on the downing of the Malaysia Airlines flight that was found to largely lie outside our diplomatic category, we assess TASS reporting on Freedom House as lying squarely within the information category. Freedom House's explicit calls for greater freedom of the press, decreased censorship, and increased freedom to access information drew a more negative response from TASS reporting than any other action threatened or undertaken in any of the other three categories. Diplomatic criticism, economic sanctions, nor even military exercises undertaken by NATO in Eastern Europe created as negative a reaction as Freedom House reporting by TASS.

¹⁴⁶ Freedom House, *Reports*, <https://freedomhouse.org/reports>, accessed 29 January 2017.



*Figure 4: TASS reporting on Freedom House;
P=positive, P+ is very positive; N is negative and N+ is very negative.*

As mentioned above, the second image, below, illustrates how the negative feeling was maintained at a relatively steady level throughout the time period examined. One large set of very negative (or positive) sentiment can alter the overall ratio, but the chart below illustrates that is not the case here.

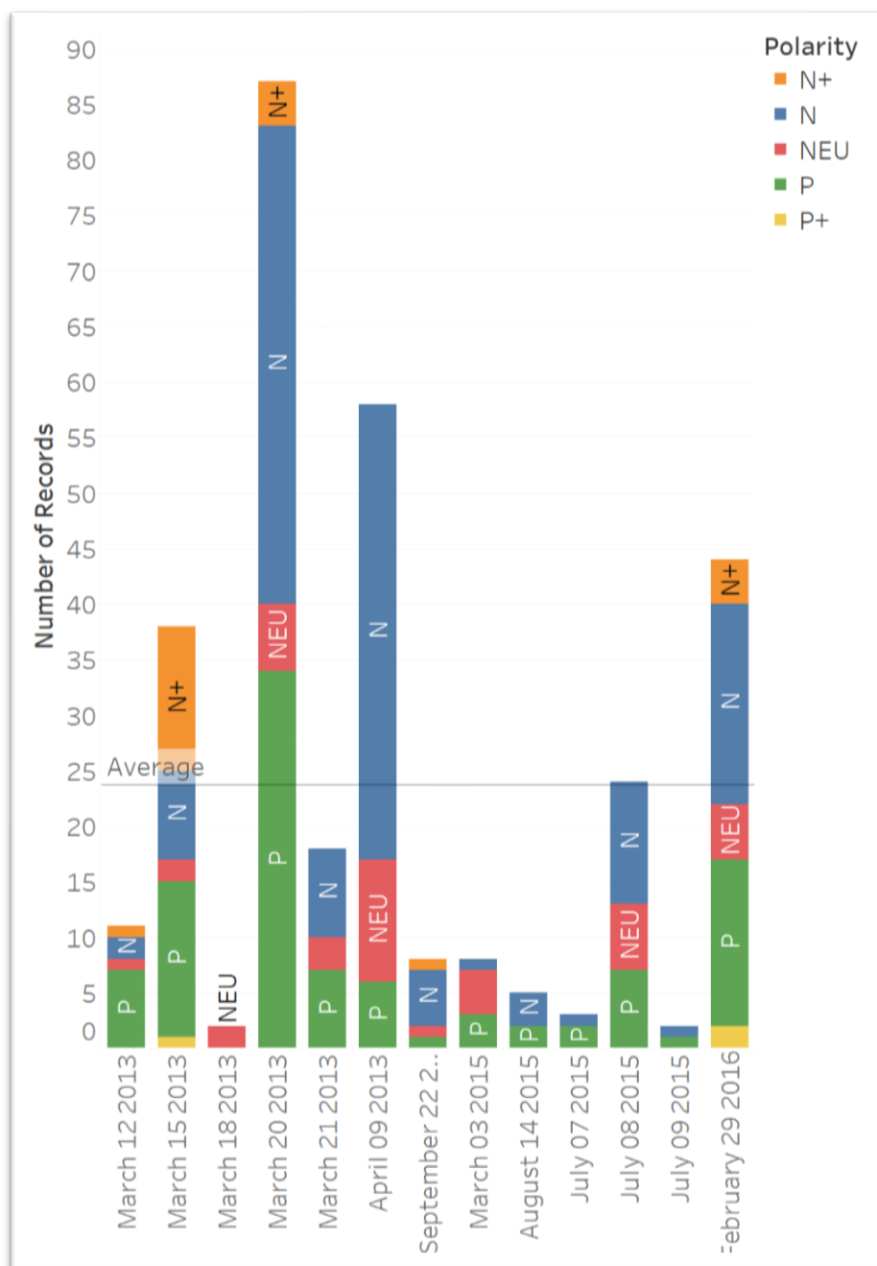


Figure 5: TASS reporting on Freedom House, 2013-2016

Also of interest, while TASS reports on Freedom House were garnering such negative sentiment, TASS reports on findings announced by Reporters without Borders took a different approach. TASS avoided all mention of Russia in stories about Reporters without Borders findings, instead all media reports on the subject

refocused attention on conditions in *other* countries. Specifically, the focus changes depending on which country Russia was in conflict with at the time – during the conflict with Georgia, TASS stories on Reporters without Borders findings focused on Georgia’s poor standing. During the conflict with Ukraine, that country’s poor performance in the rankings became the focus of TASS reporting. In between the Georgia and Ukraine conflicts, issues with U.S. performance drew attention.

A similar effort was made in regards to TASS reporting on the annual release of the U.S. State Department’s report on human rights. Of the 11 reports found on TASS during the search period, only one was about Russia’s standing in the report. All of the other stories focused on U.S. criticisms of other countries, with Ukraine once again drawing the lion’s share.

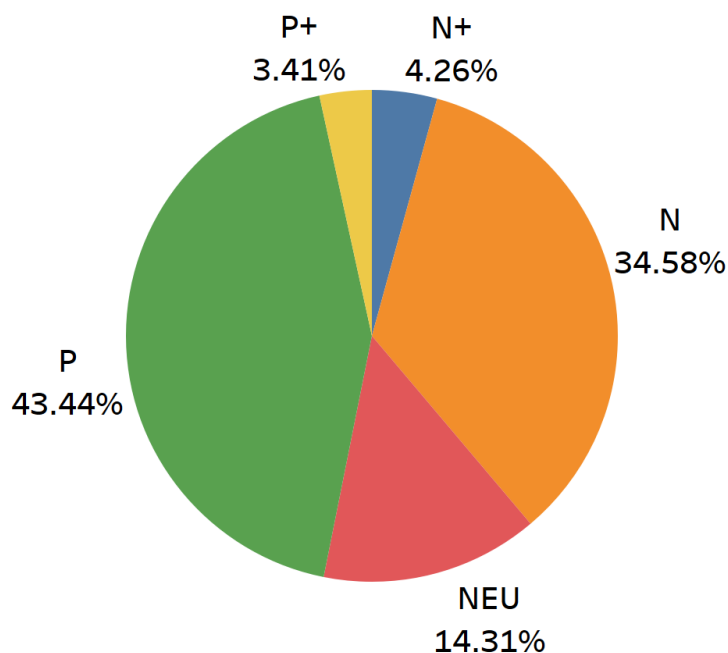
In short, TASS reports on Freedom House findings, including related criticism of Russia’s lack of freedom in the information environment, displayed some of the strongest negative sentiment of any topic surveyed, handily beating events from the military and economic categories, plus events from the diplomatic category aside from the somewhat unique case of the downed Malaysian jet.

TASS stories on Reporters with Borders and the annual U.S. State Department human rights report are also notable in their efforts to shift attention from criticism of Russia to criticism of countries with which Russia was experiencing poor relations or outright conflict. This finding of an active, obviously planned response was unique to the information category.

Overall, these initial findings from TASS appear to support the paper’s premise that countries restrictive of their domestic information environment

possess heightened sensitivity to challenges that threaten those restrictions. If, as is demonstrated here, threats to information controls are perceived more negatively (and generate a more active response), than threats in the other three categories, then the saliency of information as an effective foreign policy tool increases.

The third most negative set of comments, also from TASS, is where positive sentiment exceeds negative sentiment for the first time (47% positive to 39% negative), per the image below. This event brings us into the economic category, focusing on U.S. economic sanctions applied to Russia in December 2015.



*Figure 6: TASS reporting on U.S. economic sanctions in December 2015;
P=positive, P+ is very positive; N is negative and N+ is very negative.*

As in the previous example above, the chart below illustrates how the relative levels of positive and negative sentiment were maintained throughout the period surveyed – in this case, during December 2015 as the sanctions were

discussed and applied (on 22 December). Interestingly, the EU also announced in December 2015 (on the 21st) that it would extend existing sanctions on Russia by another six months, until 31 July 2016. Note the spike in reporting on the 22nd, especially the relatively elevated levels of N+ (very negative) reporting the day the U.S. sanctions were applied and the day after the EU announcement.

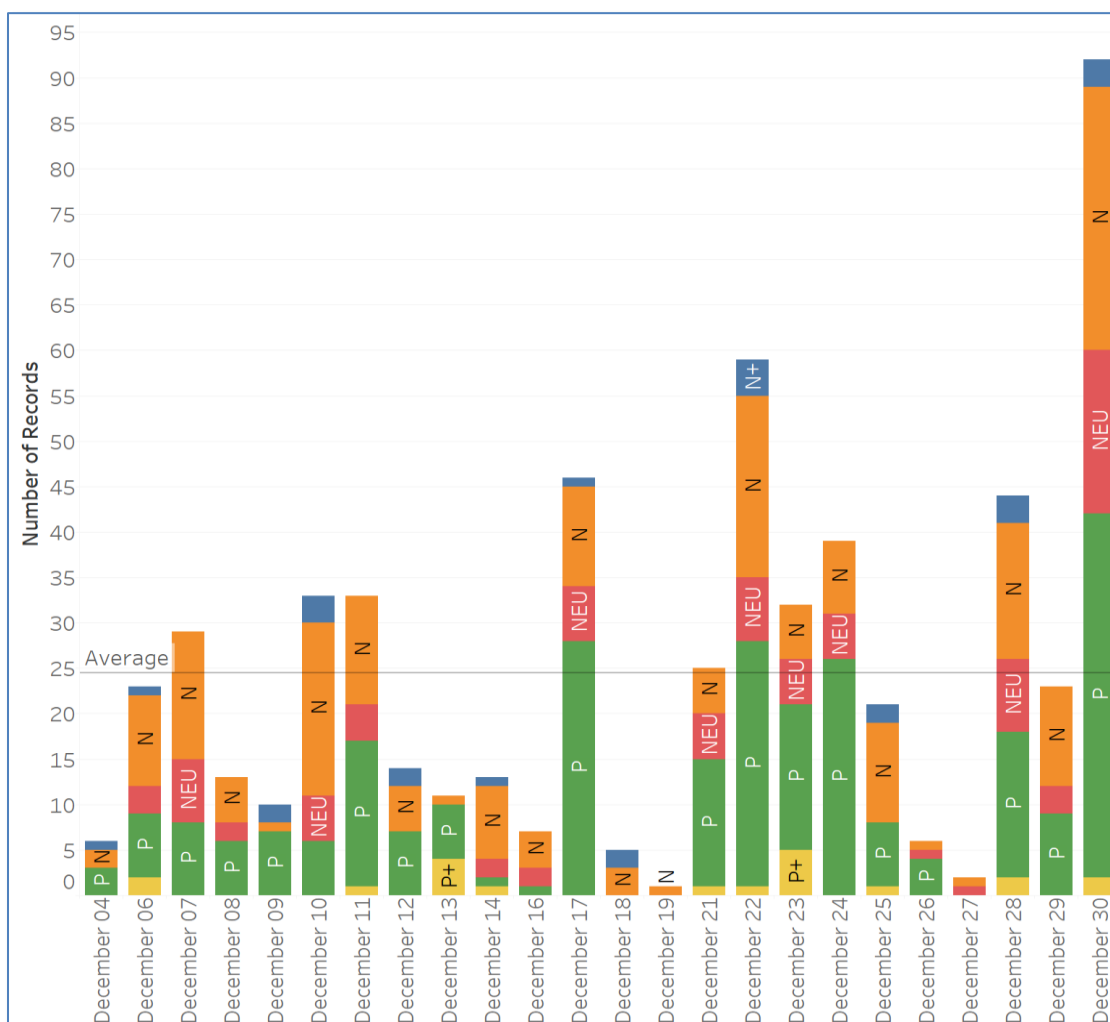


Figure 7: Timeline of TASS reporting on U.S. economic sanctions in December 2015

From the examination thus far, we have seen only two events generate greater negative than positive sentiment: the downing of the Malaysia Airlines plane

and the Freedom House reports. The third event, economic sanctions in December 2015, had a 39% negative to 47% positive ratio – relative to the other events, the sanctions generated more negative sentiment in TASS reporting, but overall the reports were more positive than negative.

The following event, TASS reporting on sanctions imposed by the U.S. and EU in March 2014 in response to the Russian invasion of Crimea, is also from the economics category, but at 31% negative to 54% positive, the threat and imposition of sanctions can hardly be deemed to have generated an overall negative response from the Russian government. So far, we have only seen TASS reporting (per above, it is more negative than MOFA reporting), but the economic category brings our first reporting from MOFA, on the December 2015 sanctions imposed by the U.S. and EU. This was not only the most negative (least positive) of the MOFA reporting, it was the only event where the TASS numbers (39% negative, 47% positive) were somewhat close to the MOFA numbers (30% negative, 54% positive).

From what we have seen thus far, no TASS or MOFA reporting in the military category generated significant negative sentiment from the Russian government. TASS reporting of the downing of the Malaysian airliner generated the most negative sentiment, though that negativity was largely focused on the downing of the plane and lives lost rather than the diplomatic repercussions. Economic sanctions generated a relatively uniform, high level of negative sentiment across both TASS and MOFA reporting, though again, the positive sentiment outweighed the negative for all events surveyed. Only the information category appeared to generate a strong effect in the reporting, with the second most negative level of

TASS reporting and an interesting, possibly salient effort to refocus attention generated by the Reporters without Borders and other reporting onto countries with which Russia was experiencing conflict or poor relations.

An important related point on negative sentiment before moving on to events with the most positive reporting – beginning in the spring of 2015, Russian government sentiment toward the U.S. government suddenly turned negative. Per the timeline below, built from GDELT data (which we’ll explore in further detail below), prior to the spring of 2015, Russian government sentiment toward the U.S. government was always positive, though occasionally veering toward neutral (e.g. February 2013). Since March of 2015 however, it has always been negative. While this represents a limited time period (1.5 years in our data), the switch is sudden and dramatic. It also colors the events under examination in this section (hence including it here).

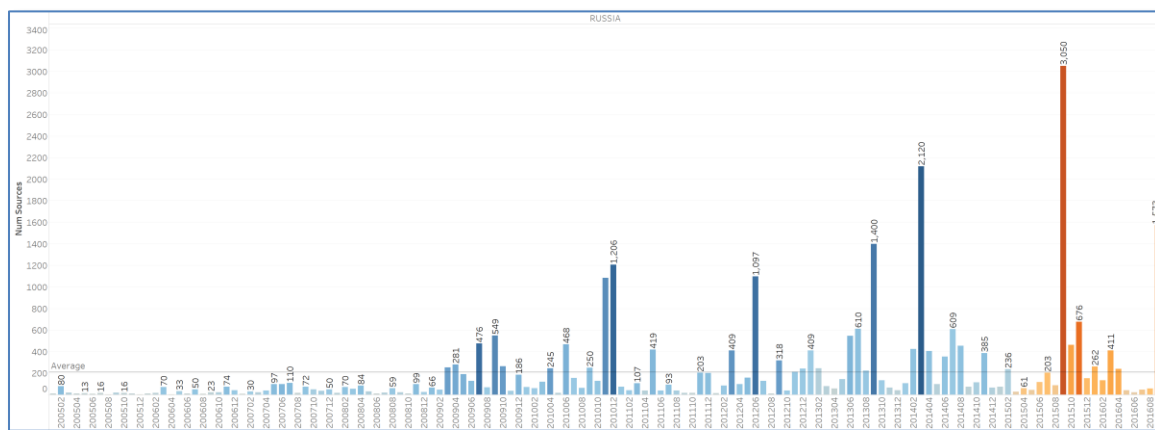


Figure 8: Russian government views of the U.S. government from 2007-2016. The bars' height represents the number of Russian sources, the higher the bar, the greater the number of sources discussing an event that month; the bars' color represents sentiment, with darker blue more positive, grey as neutral, and red as most negative.

From the image above, we can see there are relatively few sources prior to 2009. Given the difficulty of reading the timeline, we will insert the same timeline below, only with the first three years of data (2005-2008) removed. Also, per the image above, some months, even in later years, only have a few sources. In the interest of legibility, we will also take out any months with fewer than 20 sources. The resulting timeline, below, is somewhat more legible.

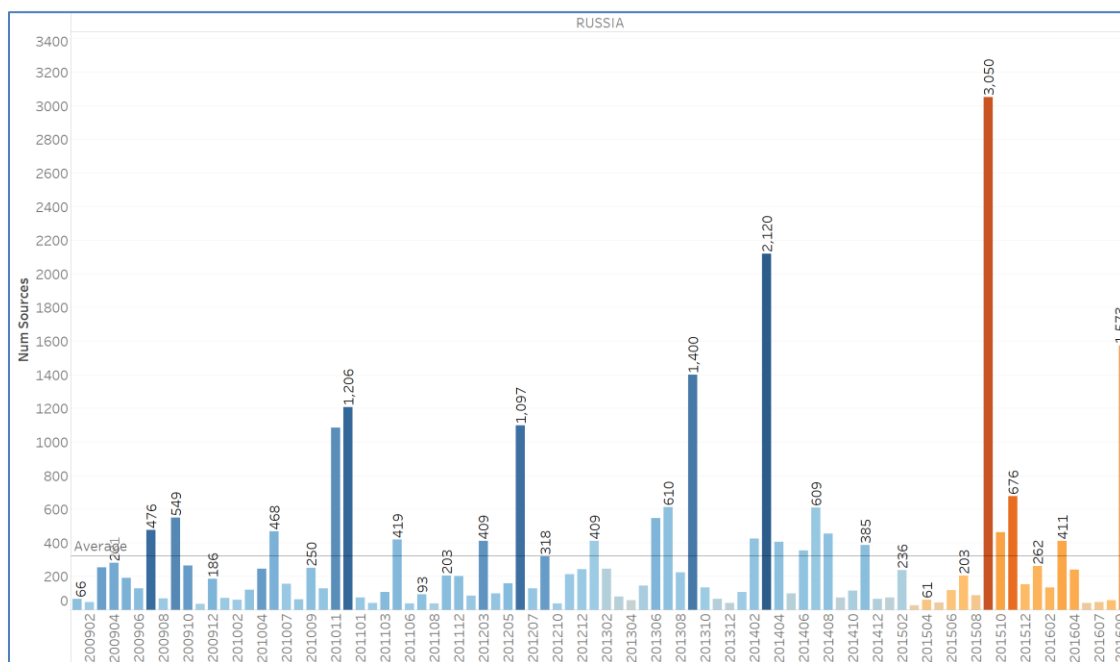


Figure 9: Russian government sentiment toward the U.S. government, 1 January 2009 to 30 September 2016.

The bars above represent Russian government interaction and sentiment toward the U.S. government as captured by GDELT in just over 24,300 rows in Excel. Each row represents one event reported by one source – the greater the number of sources in a month reflects a greater number of events in Russia-U.S. relations for that month. Essentially, the greater the number of interactions in a month, the higher the bar, the more ‘important’ the event(s) occurring that month in Russia-U.S.

relations. The color of the bar represents sentiment, the darker the blue, the more positive; the darker and redder the orange, the more negative (the Russian government sentiment toward the U.S. government).

We will explore the GDELT data in more detail below. What it means for this section is that despite overall negative sentiment by the Russian government toward the U.S. government, the December 2015 economic sanctions reporting from TASS and MOFA discussed above, while relatively negative in the context of TASS and MOFA reporting, is surprisingly positive in terms of overall Russian government sentiment toward the U.S. government at the time the sanctions were imposed (December 2015).

The GDELT data also shows that the negativity of reporting on the Malaysian Airlines flight is again an outlier, negative at a time (especially August 2014) when overall sentiment by the Russian government toward the U.S. government is positive. The information category reporting matches the negativity of the overall relationship after March 2015, but is a negative outlier in 2013 and 2014. Perhaps most interesting, as we will see below, is the military category, with TASS and MOFA reporting on NATO exercises surprisingly positively, even after overall Russian government sentiment turns negative.

Positive Sentiment

So far, we have focused on events with high levels of negative sentiment. Here we will look at the opposite end of the spectrum, at the most positive comments. Unlike TASS, the positive comments largely came from the Ministry of

Foreign Affairs and, not surprisingly, the highest levels consisted of Russian reaction in 2010 to the signing of the START Treaty with the United States. This diplomatic agreement was viewed overwhelmingly positively, with MOFA reporting a positive to negative ratio of nearly 7:1, at 74% positive to 11% negative.

Aside from this positive diplomatic story, the next five most positive events, all with over 60% positive sentiment, are, surprisingly, from the military category (note also that several 'positive events' appeared after overall Russian sentiment had soured and turned negative):

1. TASS reporting on NATO 'Trident' exercises from March 2014 to June 2016 (64% positive, 17% negative)
2. MOFA reporting on U.S. missile defense systems in Eastern Europe in 2007 (65% positive, 18% negative)
3. MOFA reporting on the Baltic nations joining NATO in 2004 (69% positive, 21% negative)
4. MOFA reporting on NATO exercises from 2010-2016 (61% positive, 23% negative),
5. MOFA reporting on NATO ships entering the Black Sea in 2008 during the Russia-Georgia conflict (61% positive, 24% negative).

TASS reporting on the NATO 'Trident' exercises¹⁴⁷ was not only positive at a time when Russian government sentiment toward the U.S. government had become

¹⁴⁷ For example: *Rapid Trident* in Ukraine and *Trident Juncture* in/around/above multiple NATO countries; the unique use of the term *trident* provides an easily searchable, specific proxy for military

negative, it is also the only TASS reporting measured here that is more positive than MOFA's reporting. To put it clearly, aside from this one event, all TASS reporting displayed more negative sentiment than all MOFA reporting.

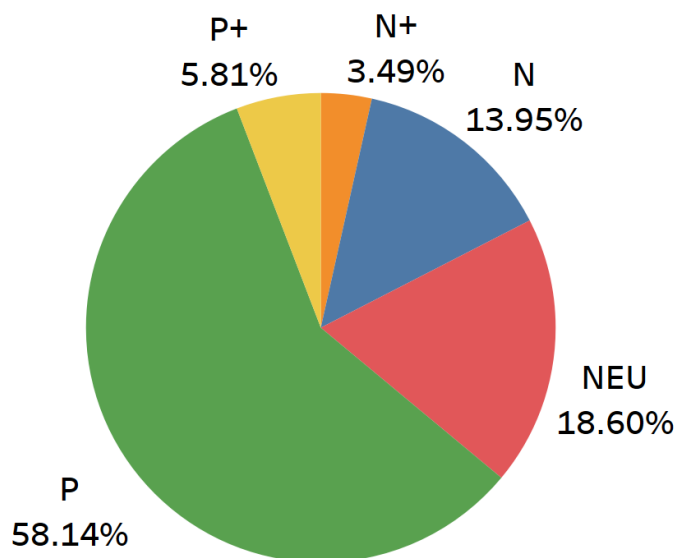


Figure 10: TASS reporting on NATO's Trident Exercises is, at 64% to 17%, surprisingly positive.

The MOFA reporting comprises the next four most positive stories, again, all of which fall into the military event category. Next is MOFA's reporting on the 2007 decision by the United States to proceed with putting missile defense systems in Eastern Europe, systems ostensibly designed to protect Europe from Iranian nuclear missiles rather than Russian missiles.

exercises. The broader phrase "NATO exercise" was also used, per above, and produced broadly similar results.

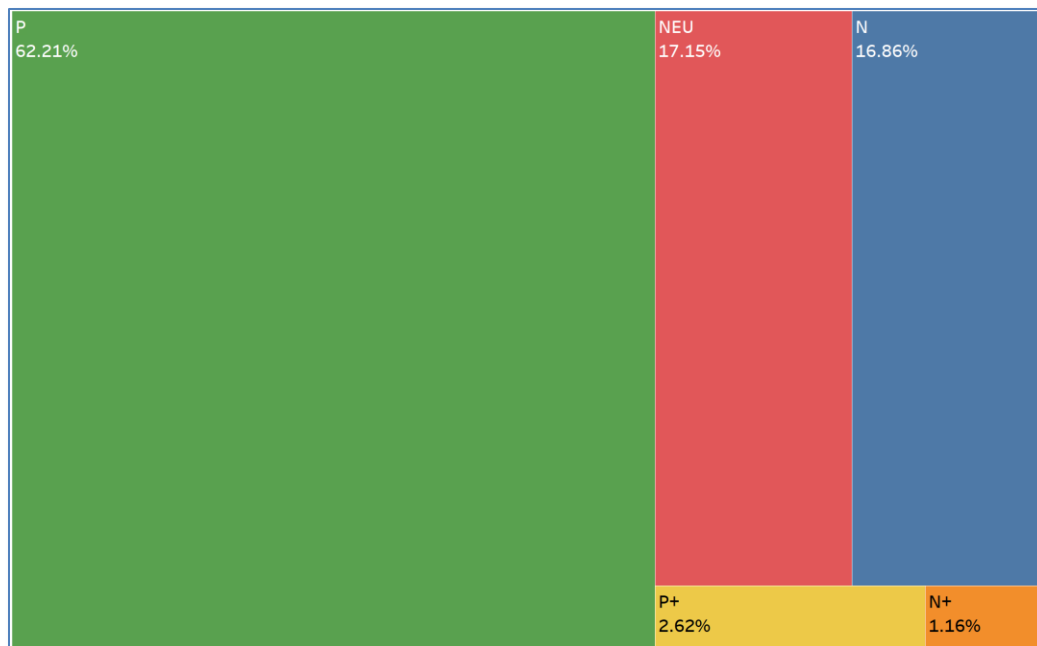


Figure 11: MOFA's largely positive response to the U.S. decision to base anti-missile defenses in Eastern Europe.

The fourth most popular, interestingly, focused on MOFA's reaction to the Baltic states (Estonia, Latvia, Lithuania) joining NATO in 2004. We explored this, relatively dated, factor as a way of assessing how the Russian government reacted to military pressure, in this case the expansion of NATO past Eastern Europe and right up to the Russian border. While overall U.S./EU-Russia relations were more positive in 2004 than in recent years, the relatively high level of positive sentiment for a powerful foreign military organization allying itself with Russia's neighbors (and formerly subjugated states) is striking. Note the overall positive sentiment is three times greater than the overall negative sentiment.

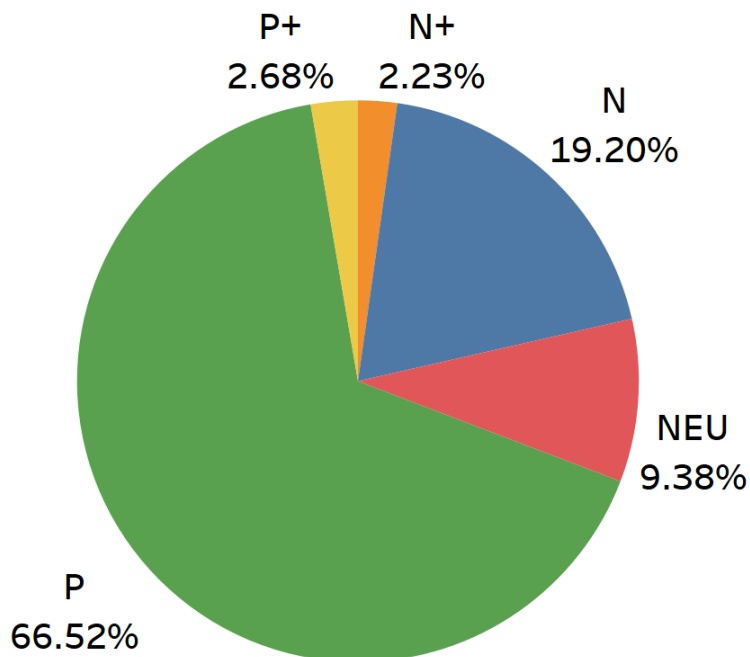


Figure 12: MOFA's reaction to the Baltic states (Estonia, Latvia, Lithuania) joining NATO in 2004.

The timeline, below, adds further details to MOFA's commentary on the Baltics officially joining NATO. Now, this NATO expansion is widely cited in Russian media as a reason for distrust of NATO and the U.S. – the expansion is highlighted as an example of how a weak Russia was forced to do nothing while NATO and the U.S. abrogated an earlier agreement not to expand NATO into Eastern Europe or the lands of the former USSR. Though, as we can see in the pie chart above and timeline below, Russian government commentary at the time was largely positive.

Though somewhat skewed by a large number of reports on 18 March 2004, the overall positive-negative ratio holds steady throughout the time period examined (March-April 2004). All three Baltic states officially became members of NATO on 29 March 2004.

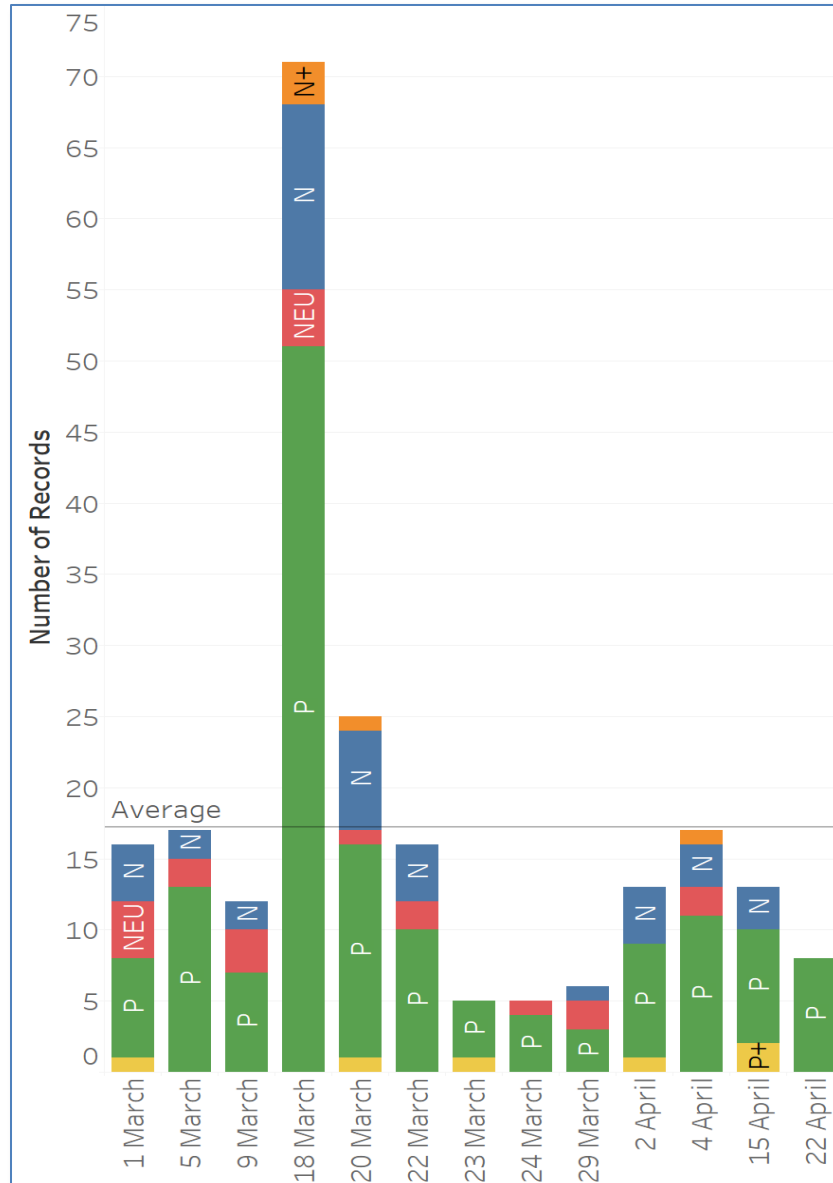


Figure 13: Timeline showing MOFA sentiment toward NATO expansion into the three Baltic states in 2004.

As mentioned above, the next two most positively-viewed events are also from the military category:

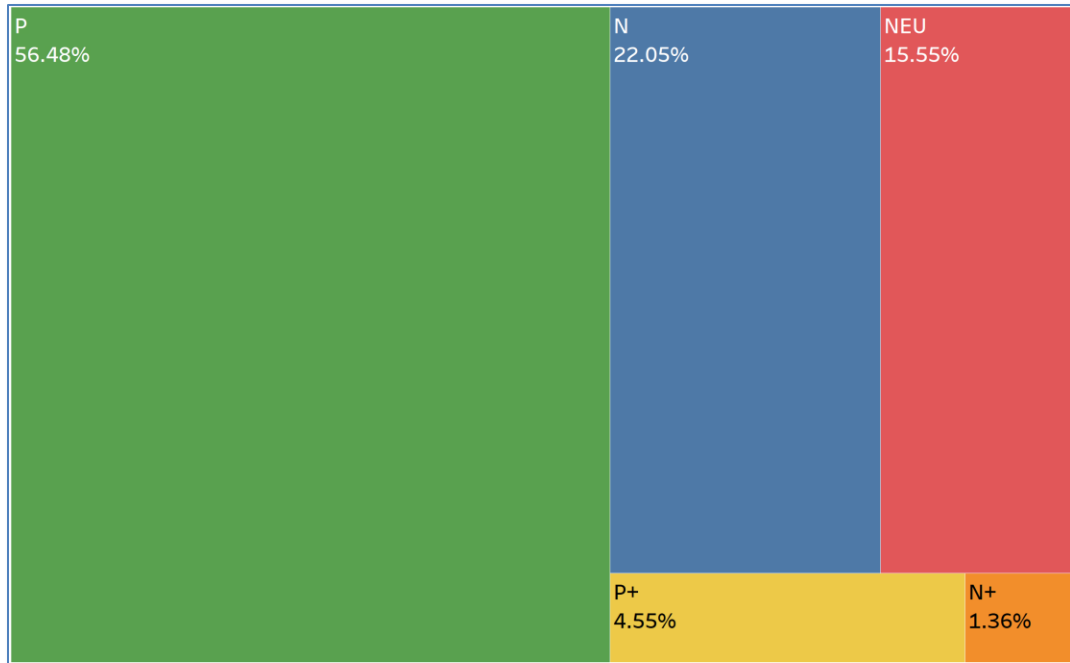


Figure 14: MOFA's sentiment toward NATO exercises, 2010-2016.

The ratio of MOFA's positive-negative sentiment toward NATO exercises remained roughly the same from January 2010 to September 2016. However, we can see from the timeline below that starting in the spring of 2014, the amount of MOFA's commentary on NATO exercises suddenly and dramatically decreased, without recovering.

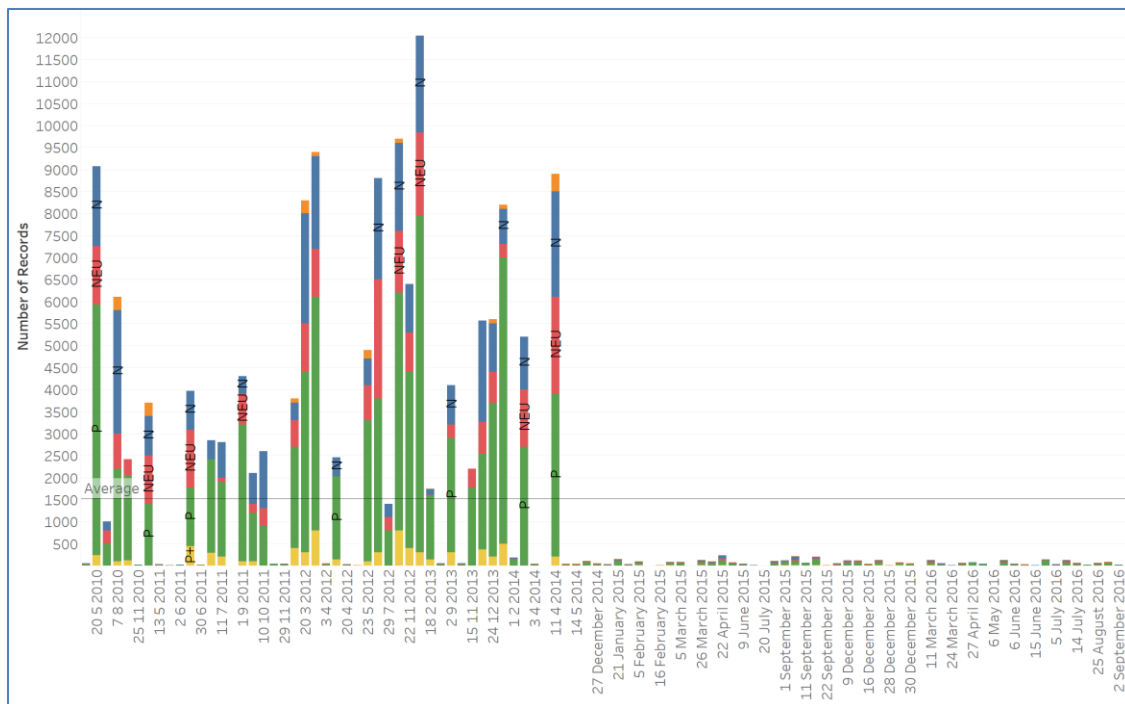


Figure 15: Note the sudden, sharp decrease in MOFA commentary on NATO exercises beginning in the spring of 2014.

The reason for this sudden, steep, sustained decrease is unclear and comes roughly a year before the change in overall sentiment from positive to negative noted above. The change may be a coincidence, the sign of a decision to decrease attention to the issue, an error in data collection, greater focus by MOFA on other issues, or a combination of these and other reasons.

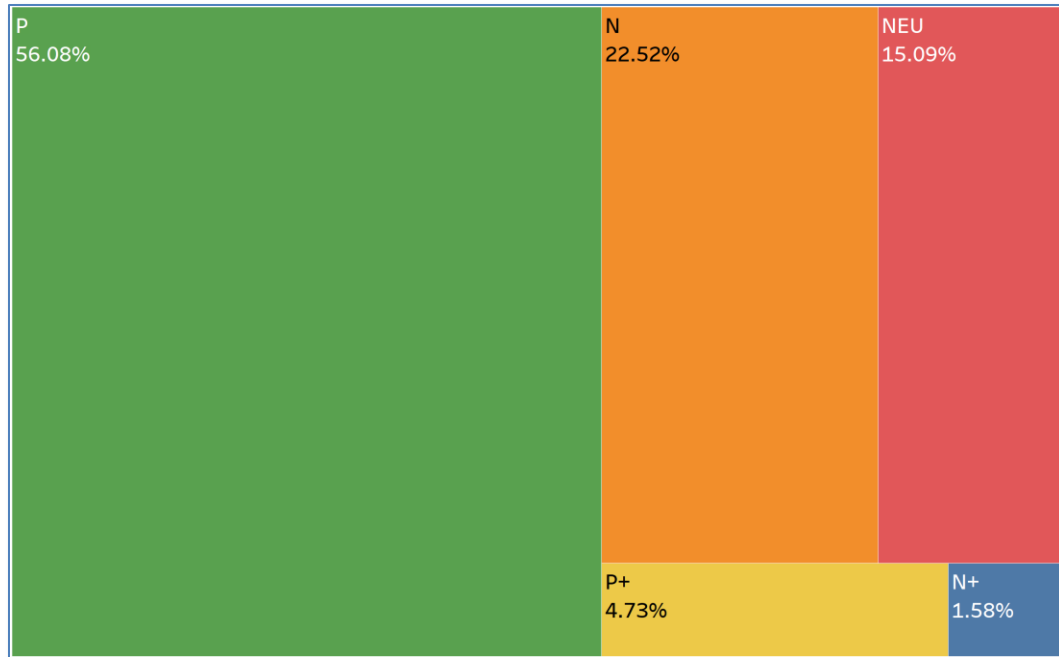


Figure 16: MOFA's sentiment toward NATO naval vessels entering the Black Sea during the conflict with Georgia in August 2008.

The final event we are examining is also military-related, the dispatch of NATO naval vessels to the Black Sea in 2008 during Russia's conflict with Georgia. While this was still a time of generally positive sentiment in U.S.-Russia relations, the positive-negative ratio is still surprising, given presumed Russian sensitivities to foreign naval vessels entering this 'near-abroad' region. A similar NATO effort today, given the current state of relations and 2015 change in the overall positive-negative sentiment ratio, would likely generate a far more negative response.

The table below provides the entire list of events, with overall negative and positive sentiment. The most negative events are at the top, most positive at the bottom.

TASS Malaysian Airliner	68% negative	24% positive
TASS Freedom House	54% negative	33% positive
TASS U.S. Economic Sanctions DEC2015	39% negative	47% positive
TASS Econ sanctions FEB-APR2014	31% negative	54% positive
TASS Crimea	31% negative	59% positive
MOFA Economic Sanctions NOV2015-JAN2016	30% negative	54% positive
MOFA Malaysia Airliner	29% negative	55% positive
MOFA OCT 2015 NATO Drills	28% negative	57% positive
MOFA Human Rights Reports	26% negative	60% positive
MOFA reacts UN Crimea 2014	25% negative	53% positive
MOFA NATO ships Black Sea	24% negative	61% positive
MOFA 'NATO' & 'Exercise' 2010-2016	23% negative	61% positive
MOFA Baltics join NATO MAR 2004	21% negative	69% positive
MOFA Missile Defense 2007	18% negative	65% positive
TASS 'Trident Exercise' MAR2014-JUN2016	17% negative	64% positive
MOFA START Treaty	11% negative	74% positive

Table 1: Event list and sentiment analysis for Russia

The findings that the downing of the Malaysian airliner and the signing of the START Treaty ranked as the most negative and positive events, respectively, in our research, support the efficacy of our methodology. Had a plane crash not ranked highly negative, or the diplomatic agreement highly positive, it would have called into question our research tools and methodology. As this is clearly not the case, we assess these findings as supportive of the validity of the methodology and toolset.

All of the findings above are based on stories/reports posted to the websites of MOFA and TASS. But what about social media? In an effort to examine this

question, the research next examined MOFA's Twitter feed (@mfa_russia, https://twitter.com/mfa_russia). Below is the overall sentiment of the Ministry's tweets for the period examined.

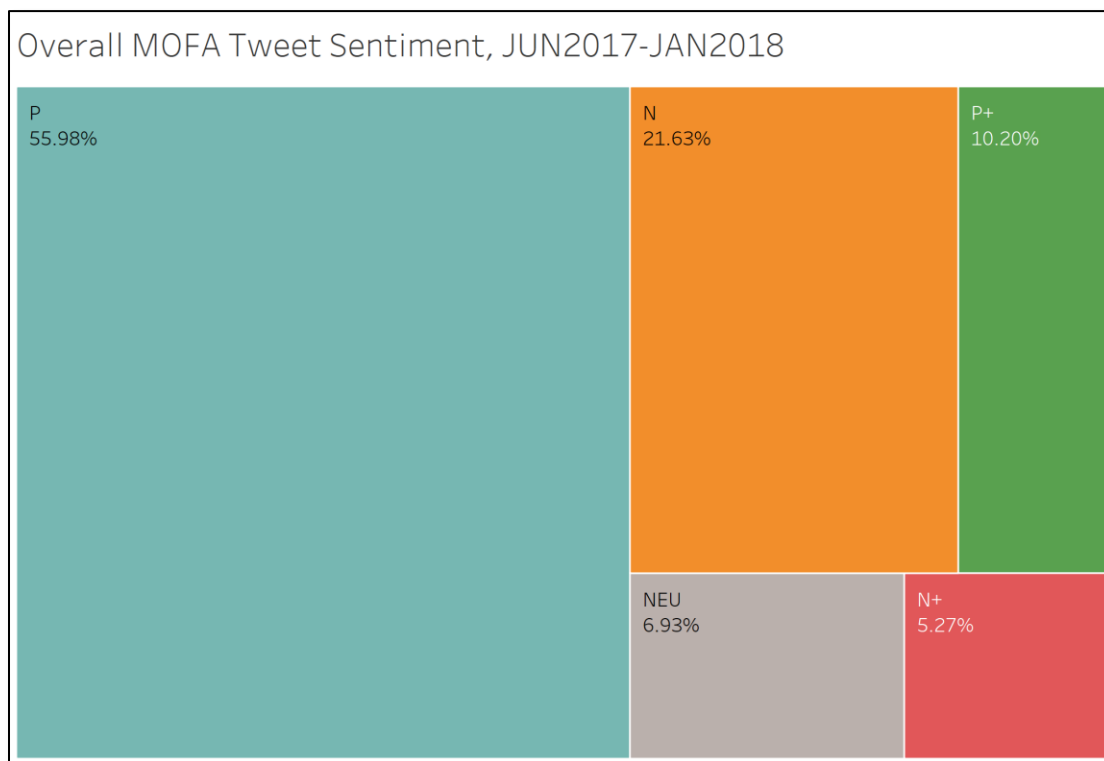


Figure 175: Overall MOFA Tweet Sentiment

Here we can see predominantly positive sentiment, with overall negative sentiment at 27%, compared to overall positive at 66%. The issue however, is the timeline. Twitter only allows access (for most researchers unaffiliated with Twitter) to an account's 3,200 most recent tweets, which meant for an organization as active on Twitter as Russia's foreign ministry, only approximately 7.5 months' worth of data was available. In addition, many of the tweets included a link to the full story/report on the organization's website – meaning the data was not so much newer or added as it was simplified and repackaged into a 140-character tweet with

a link. By only being able to go back seven months, many of the search terms used above were unavailable or had so few references as to provide little research value (e.g. only two mentions of ‘NATO exercises’ and no mentions of specific NATO exercises like Anakonda or the Trident set of exercises).

The only terms that produced enough results were *sanctions* (which were curated to remove references to sanctions for third countries like Venezuela or North Korea) and the very broad term *NATO*. Graphs of both are posted below, along with one featuring MOFA’s coverage of Zapad 17, a joint Russian-Belarusian military exercise that took place in September 2017 in nearby regions (i.e. close to the Ukraine and NATO member states) of both countries.

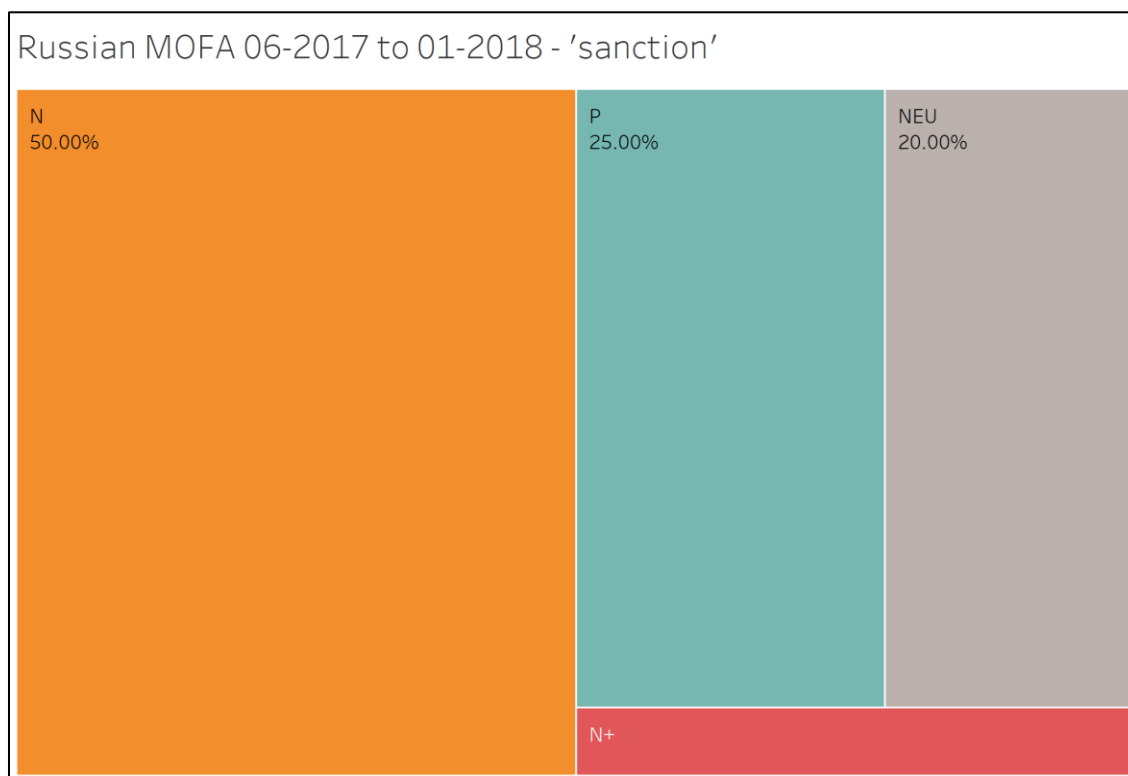


Figure 186: Russian MOFA sentiment 06-2017 to 01-2018 – ‘sanction’

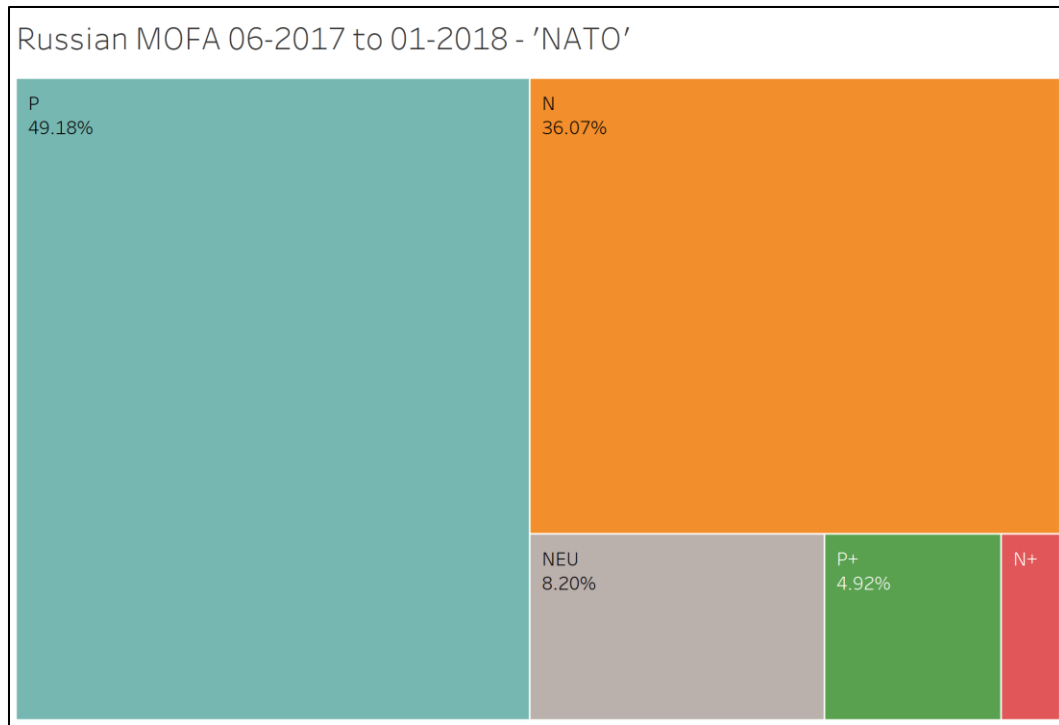


Figure 197: Russian MOFA sentiment 06-2017 to 01-2018 – 'NATO'

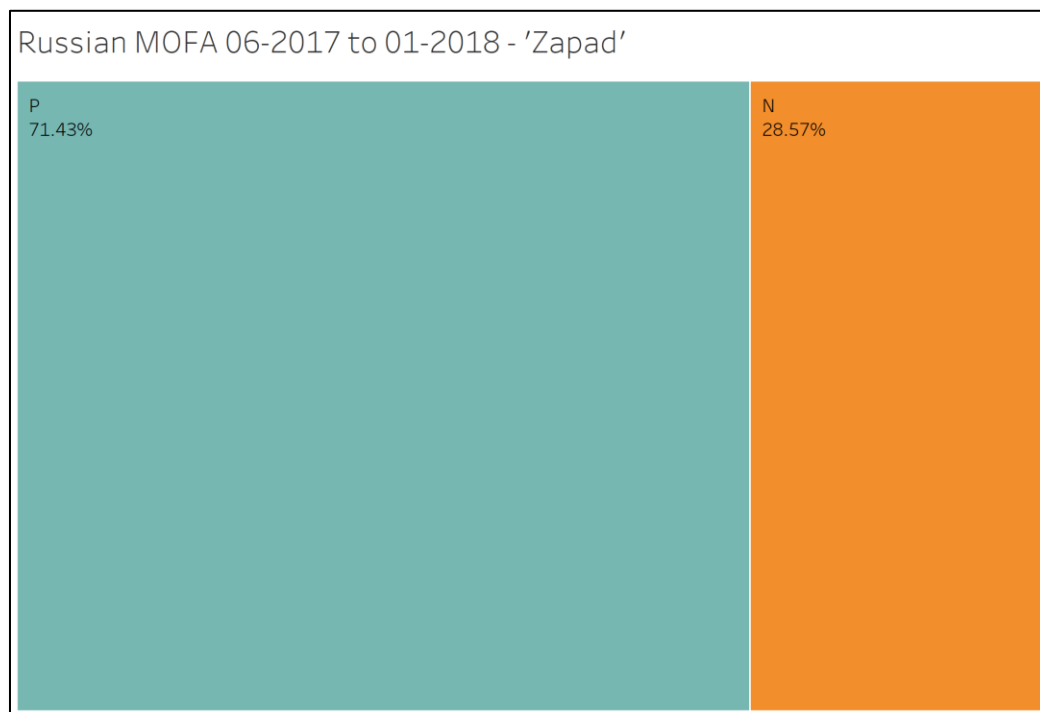


Figure 208: Russian MOFA sentiment 06-2017 to 01-2018 – 'zapad'

From these graphs, we can see MOFA's tweets in reaction to sanctions were considerably more negative (overall 55% negative) compared to the MOFA website reporting above (31% negative). However, a spike in coverage of U.S. sanctions efforts by Congress during the summer of 2017 (outside of the search/date range for the MOFA website research, above) likely drove the increased negative coverage.

The positive coverage of NATO, at 55%, is relatively similar to that found in the MOFA website searches. The comparison example, of Russia's own Zapad 17 military exercise, was 71% positive; this exercise was included primarily as a check on methodology and was expected to be highly positive.

The results above provide examples from the military and economics categories but, perhaps due to the restricted timeline, the research was unable to find results applicable to the information and diplomatic categories. Coupled with the number of tweets that included a link to MOFA's website for the report's complete text – data already available through the research methods harnessed above, social media postings provided little added value. Research able to take full advantage of Twitter's database, beyond the 3,200-tweet limit, might provide value unavailable here. In addition, one of the main advantages of social media research, illuminating networks and information flows, is not part of this current research.

TASS and MOFA Conclusion

This section provided several notable takeaways:

- Military category events were, surprisingly, among those generating the most *positive* sentiment in both state media (TASS) and official government (MOFA) reporting.
- The spring 2014 sudden and dramatic reduction in MOFA's coverage of NATO military exercises.
- The sudden negative change in overall Russian government sentiment toward the U.S. government starting in 2015 – a change that has yet to revert to previous norms.
- Social media, in the form of tweets by the Russian Foreign Ministry, provided little data not already available, in richer detail, on MOFA's website
- Finally, and most importantly for this paper, were the two findings in the information category: the strongly negative sentiment of TASS reporting on Freedom House, and the effort to refocus attention from related reporting (e.g. Reporters without Borders) onto countries with which Russia was experiencing poor relations or outright conflict.

Overall, these initial findings indicate that Russia reacts most strongly to events in the information category, least strongly to events in the military category and on balance, events in the economic category are regarded more negatively than those in the diplomatic category. Based on these preliminary findings, the Russian government is assessed as more likely to respond negatively to a future threat in the

information environment than to, for example, a NATO military exercise or the imposition of additional economic sanctions.

While these findings are preliminary and based on a limited number of events, they are utterly counterintuitive – the military category was expected to generate the most negative sentiment and strongest responses. Instead, it was the information category that generated unique response measures and the most negative sentiment. To see if this unexpected finding holds across a larger number of events, in both English and Russian, and under a different (and likely more advanced) sentiment analysis system, we now turn to the GDELT data.

SECTION 2: GDELT

The GDELT data we examined above has already provided one key insight, the sudden negative change in Russian government sentiment toward the U.S. government in early 2015. Prior to that, even during periods of increased tension, overall Russian government sentiment toward the U.S. government remained positive. As a reminder for the reader, a copy of that timeline is inserted below.

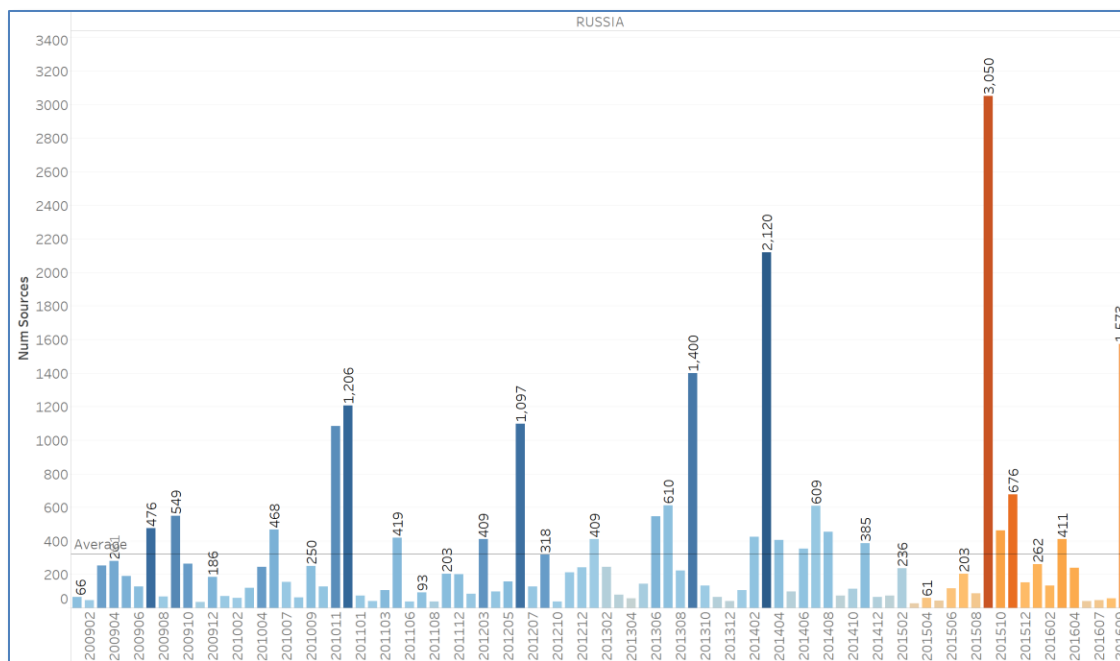


Figure 1921: Russian government sentiment toward the U.S. government, 1 January 2009 to 30 September 2016.

Why the sudden (and ongoing) change in overall sentiment? While the author of this paper is by no means a Russia specialist, there are several possible explanations. First, beginning in the fall of 2014, the value of the ruble against the dollar began a steep slide, losing nearly 50% of its value by January 2015. This came after the U.S. and EU imposed new sanctions on Russia in the late summer of 2014 in response to the downing of the Malaysian airliner discussed above. However, as the ruble regained strength in the spring of 2015, Russian government sentiment toward the U.S. government continued to worsen, undermining the argument that the value of the ruble, and the sanctions from late summer 2014, were the driving factors in either the initial change in sentiment or the continued negative sentiment.

Aside from the sanctions and value of the ruble, another possible explanation for the change in sentiment is the price of oil, a key factor in Russia's economy. Oil

prices dropped throughout the latter half of 2014, rose over the first half of 2015, then decreased again over the second half of 2015, before slowly rising throughout most of 2016. Comparing the changes in oil prices to the sentiment timeline above shows little correlation between changes in oil prices (e.g. rising over the first half of 2015) and Russian government sentiment toward the U.S. government (e.g. turning negative in the first half of 2015). Similarly, a steep decrease in oil prices during the financial crisis of 2008 had little correlation with Russian government sentiment toward the U.S. government.

With oil prices and the value of the ruble largely ruled out as the causal factors for the sudden sentiment change, whither the four categories of foreign policy tools under examination here? Is one of them perhaps the cause of this change in sentiment?

To that we now turn, with an examination of the GDELT data broken down into the four categories. Unlike the section above however, the GDELT data is not centered around specific events. Rather, it looks more broadly at the use of each of the four foreign policy tools from 1 January 2005 to September 30 2016, then compares these findings with the by now familiar timeline of Russian government sentiment toward the U.S. government.

Military

Since the results of the military-related category were so surprising above, we will look at that category first. The chart below shows reporting on U.S. government military-related events (from threats to NATO drills) targeting Russia between 1 January 2005 and 30 September 2016. The darker the blue, the more positive the sentiment; the darker/redder the orange, the more negative the sentiment. For greater legibility, only months with at least two sources are included.

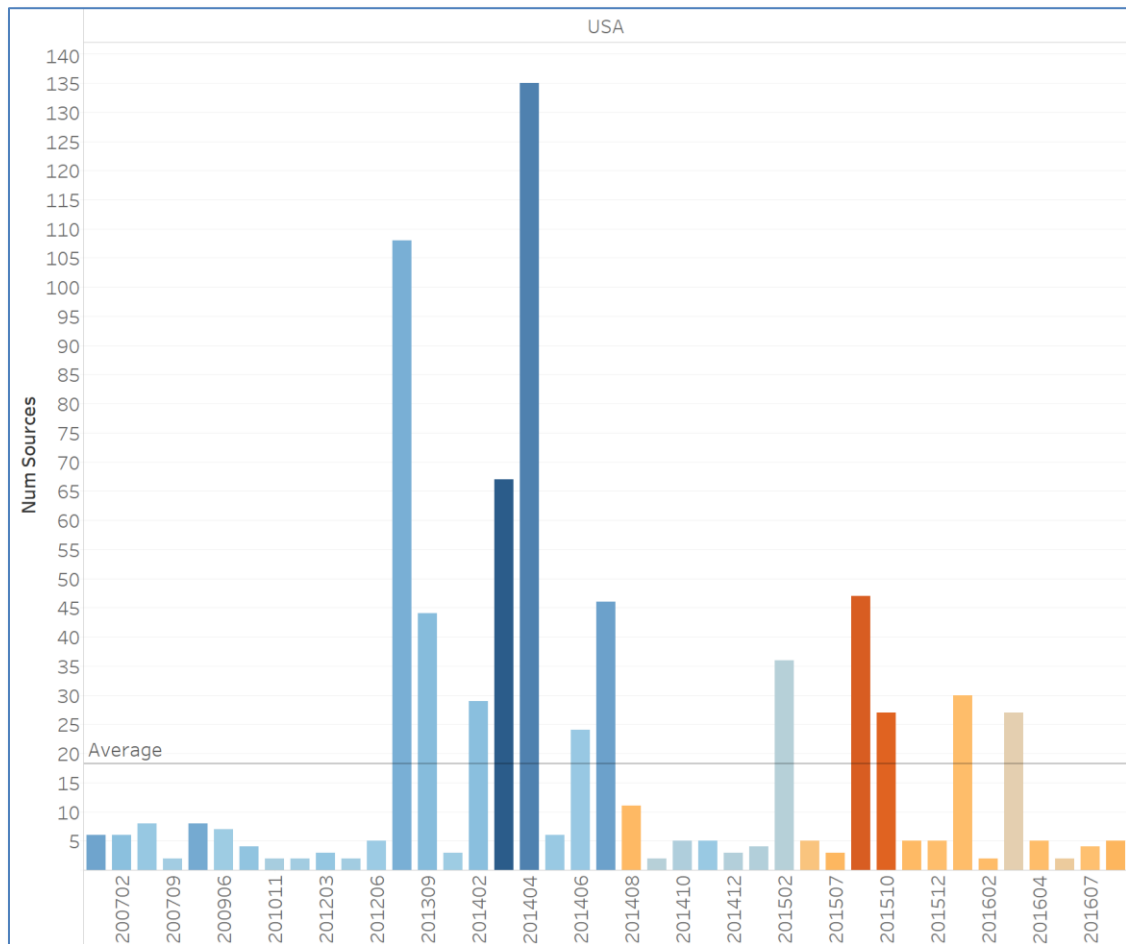


Figure 20: U.S. government military threats and actions toward the Russian government, broadly categorized.

From the timeline, we can see that the months with the greatest number of sources are in 2013 and 2014 (though not clearly labeled in the timeline, August 2013 has the second highest number of overall sources), and are positive in sentiment. Sentiment first goes negative in August 2014 (the Air Malaysia downing in July 2014 brought increased attention from NATO to the situation in eastern Ukraine),¹⁴⁸ then reverts to slightly positive from September 2014 to February 2015, after which it remains negative.

The GDELT ontology allows for both broad and narrow classification of events. The chart above is broad, using terms like *threat*, *fight*, etc. that encompass not only the military category but may also include elements from other categories (e.g. both the threat of economic sanctions and the threat to use military force are found under the broad term *threat*). The chart below is much more narrowly defined, containing only specifically military-related events. As above, for purposes of legibility, only months with at least two related sources are shown.

¹⁴⁸ See, for example, Breedlove and Rasmussen, the Supreme Allied Commander Europe and NATO Secretary General, respectively, "A NATO for a Dangerous World," August 18, 2014, and additional commentary in the archives of the Supreme Headquarters Allied Powers Europe at <http://www.shape.nato.int/2014>.

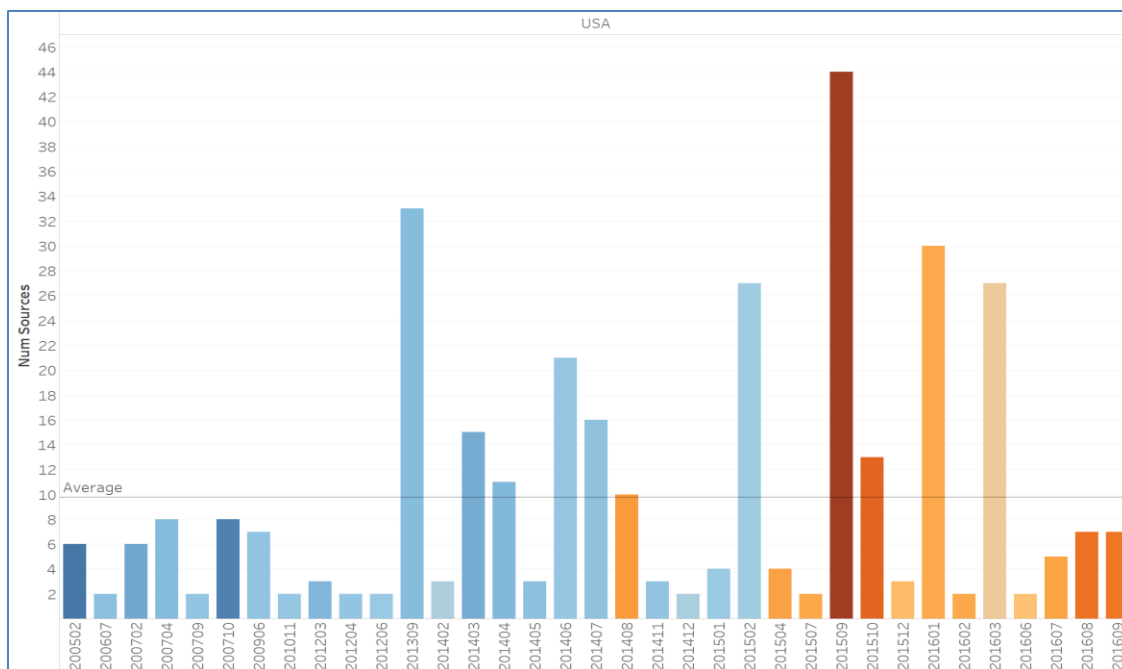


Figure 21: U.S. government military threats toward the Russian government, Feb. 2005 to Sep. 2016.

As we can see from the timeline, the focus on military-only events reduces the number of months and sources with positive sentiment, holds to the previous patterns of starting positive but turning negative, and highlights September 2015 as having both the greatest number of sources and the most negative sentiment. Note also that the number of sources is relatively low, with the average number at 10, compared to over 100 in some of the timelines above. Also note the months-long gaps with no data, especially in the early years of the timeline.

Next, we can compare the military category timeline above with the Russian government sentiment timeline. We will insert a modified version of that timeline below, focusing on June 2012 to September 2016, the period with the highest numbers of reports.

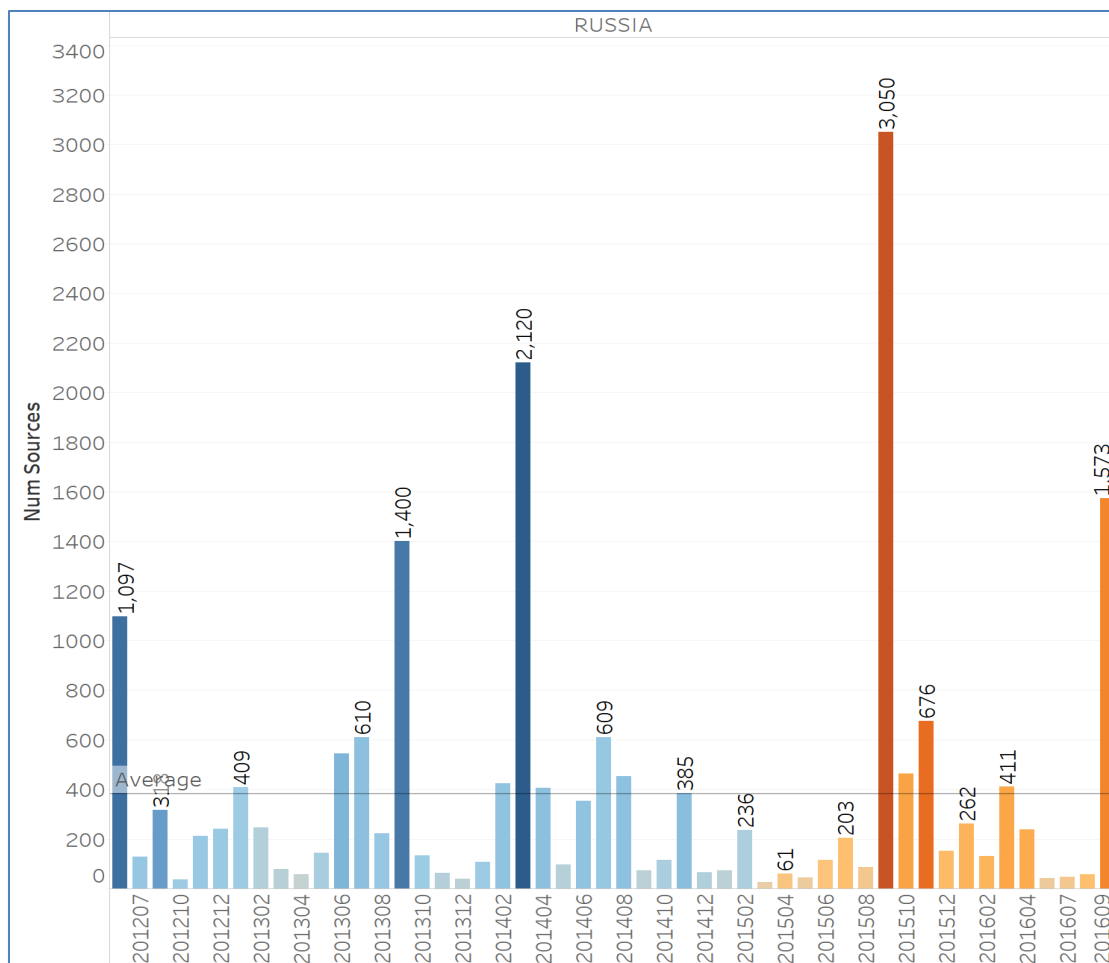


Figure 22: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016.

The first thing that leaps out from the two timelines is September 2015.

Russian sentiment is at its most negative, and sources are at their highest, the same month U.S. sources and sentiment are at their highest and most negative. This finding initially appears to support the idea that U.S. military pressure on Russia generated a strongly negative response from the Russian government.

Taking the investigation a step further however shows the correlation is likely due to the situation in Syria, not U.S. attempts to pressure the Russian government militarily. Russia dispatched warships and aircraft to Syria beginning in

August, with initial air strikes taking place on the last day of September. Both the force buildup and subsequent attacks generated significantly increased reporting, with the U.S. government criticizing the Russian buildup and the Russian government responding negatively to the outside criticism.

This undermines the initial finding that U.S. attempts to militarily pressure Russia generated the increased reporting and negative reaction. Instead, the reporting and negativity appear to reflect disagreement over an outside issue – the U.S. government was not pressuring Russia with the military tools of foreign policy, rather it was responding negatively to Russian military actions. Likewise, Russia was responding negatively to the U.S. criticism.

Removing this month from consideration greatly undermines the initial finding, that the U.S. government's use of military threats as a tool of foreign policy affected the Russian government. Instead, looking at the other months with overall negative sentiment, one can see little connection between U.S. government pressure and Russian government reaction, including during NATO's 'Trident' and other exercises in Eastern Europe, the Baltics, and Ukraine.

An outlier is August 2014, with U.S. government sentiment suddenly and briefly negative, while Russian sentiment remained positive. This was just after the downing of the Malaysian airliner, when U.S. and NATO sentiment toward Russia turned negative. The negative U.S. sentiment was short-lived however, and appeared to have little effect on Russian government sentiment, which remained positive.

On the opposite side, September 2013 provides an example of both positive sentiment and increased sources for both governments. However, as with the negative case of September 2015, the reason for the positive spike appears to be Syria, rather than a Russia-specific event. Specifically, the positive sentiment of September 2013 is likely due to an agreement between the Russian and U.S. governments over ridding Syria of chemical weapons – a proposal originally offered by Russia as the U.S. reportedly prepared for military action in Syria. Aside from this one spike, there appears to be little correlation between positive U.S. government events in the military category and Russian government sentiment.

In conclusion, this section opened with the possibility that U.S. use of the military as a foreign policy tool affected Russian government sentiment. However, further examination undermined this initial finding. The strong negative overlap in September 2015 turned out to be due to disagreement over Russian actions in Syria, not U.S. actions targeting Russia. Additionally, U.S. government military exercises with NATO occurred annually, but created no discernable pattern or effect in Russian government sentiment, either during years when sentiment was positive, or in 2015 and 2016 after Russian government sentiment had turned negative.

The mild positive overlap in September 2013 also turned out to be related to Syria, rather than U.S. government efforts to reduce military threats targeting Russia. Overall, there appears to be no evidence in the GDELT data that the U.S. government's use of the military as a tool of foreign policy had any effect, positive or negative, on the Russian government. While this conclusion is consistent with the

previous examination of TASS and MOFA reporting, it remains counterintuitive and out of step with political science orthodoxy.

Economics

Above, we briefly discussed oil prices and the value of the ruble, and found them unrelated to Russian government sentiment. In this section we turn to the economic tools of statecraft in greater detail. As in the military section, our first timeline includes the broadest possible classification of events, and also excludes months with fewer than two sources. A key point to note at the outset is that GDELT has far fewer event categories related to economics than it does to the diplomatic and military categories. This does not appear to affect the broad categorization, which contains events that overlap many of the military and diplomatic categories; the lack of diversity does however affect our narrow classification timeline (further below).

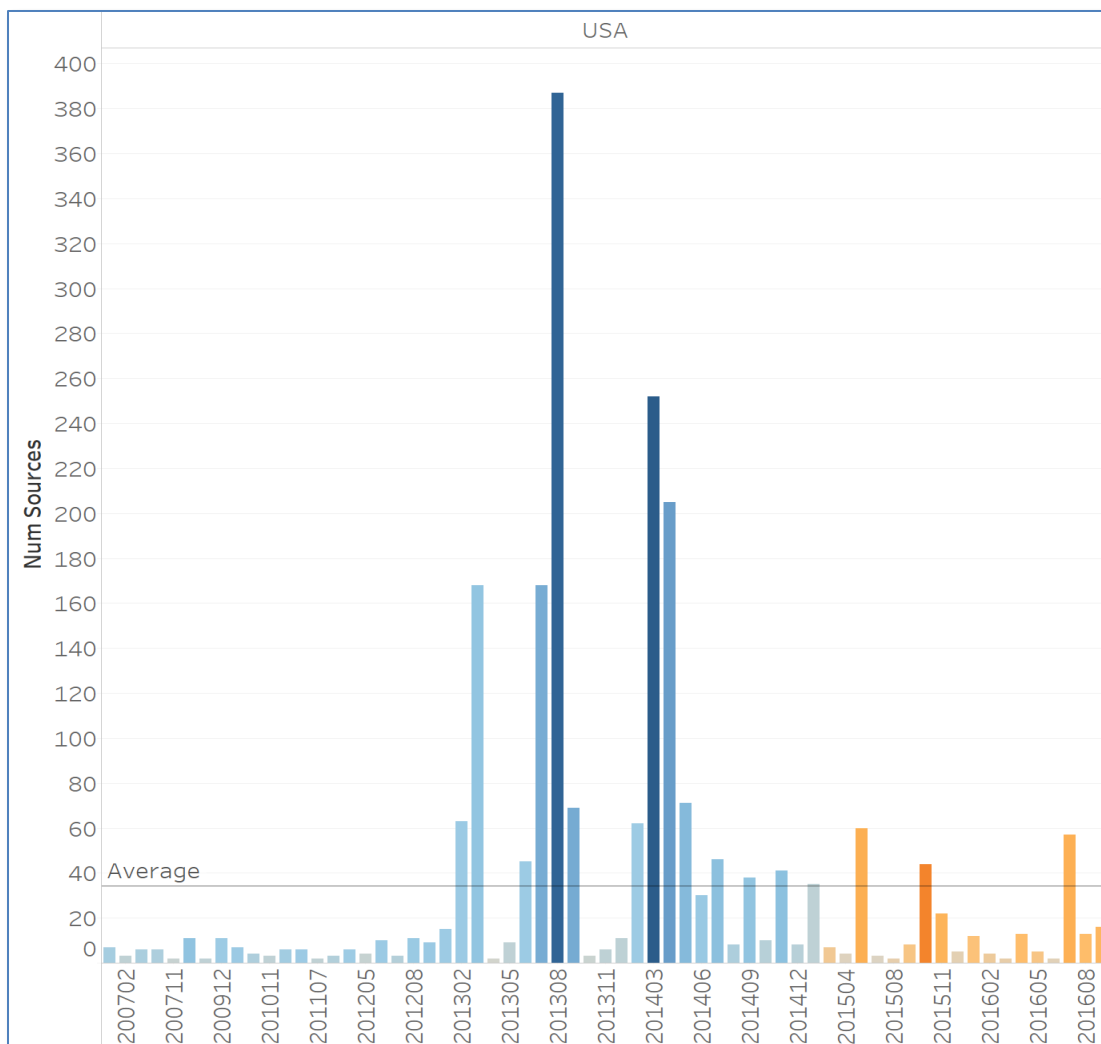


Figure 23: U.S. government economic threats and actions toward the Russian government, broadly categorized.

From the timeline, and the previous military one, we start to see that the U.S. government experienced the same overall change in sentiment, from positive to negative in early 2015, that we already discovered for the Russian government. Interestingly, the change in Russian sentiment appears to lead that of the U.S. government by two-three months.

Aside from that finding, the categorization of this timeline is too broad to draw any significant conclusions (e.g. the term *threat* includes the threat of

sanctions, the threat of military action, and the threat of a reduction of diplomatic relations). The chart below is much more focused, covering only events specifically related to the economic category. Again, the chart only includes months with two or more sources reporting on an event.

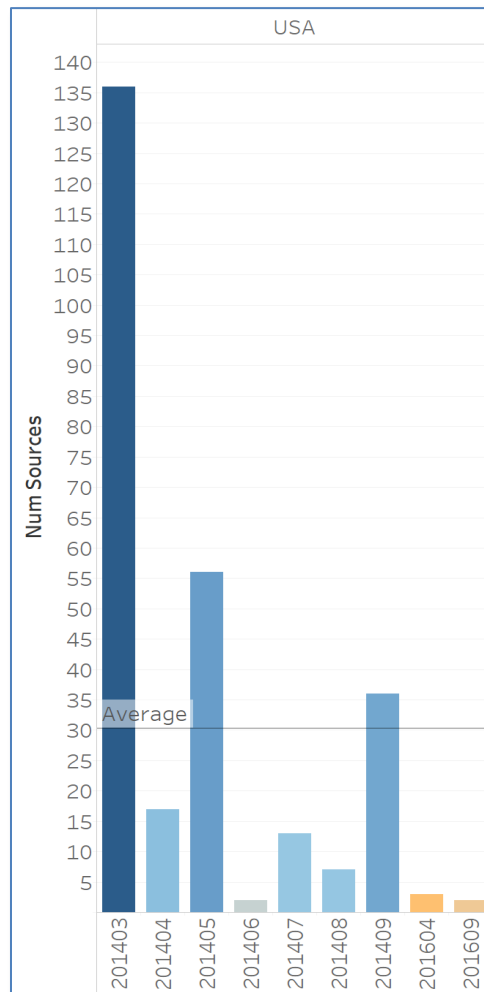


Figure 24: U.S. government economic threats and actions toward the Russian government.

The first thing that jumps out about the timeline is how thin it is – meaning, according to GDELT data, the U.S. has only threatened or actually employed economic tools directed at Russia’s government a handful of times, which we know

is incorrect thanks to the TASS and MOFA research above. A closer examination of the GDELT ontology however reveals the reason why – economic sanctions and related tools (both their threat and actual employment) are classified *not* as something done by one government to another government; instead they are classified as measures taken by one government directed at the *economy* of another state. The chart below incorporates this ontological distinction by GDELT and shows U.S. government efforts to threaten or impose the economic tools of statecraft on *Russia*, broadly defined, rather than the more specific, narrowly defined *Russian government* used in the narrower timeline above.

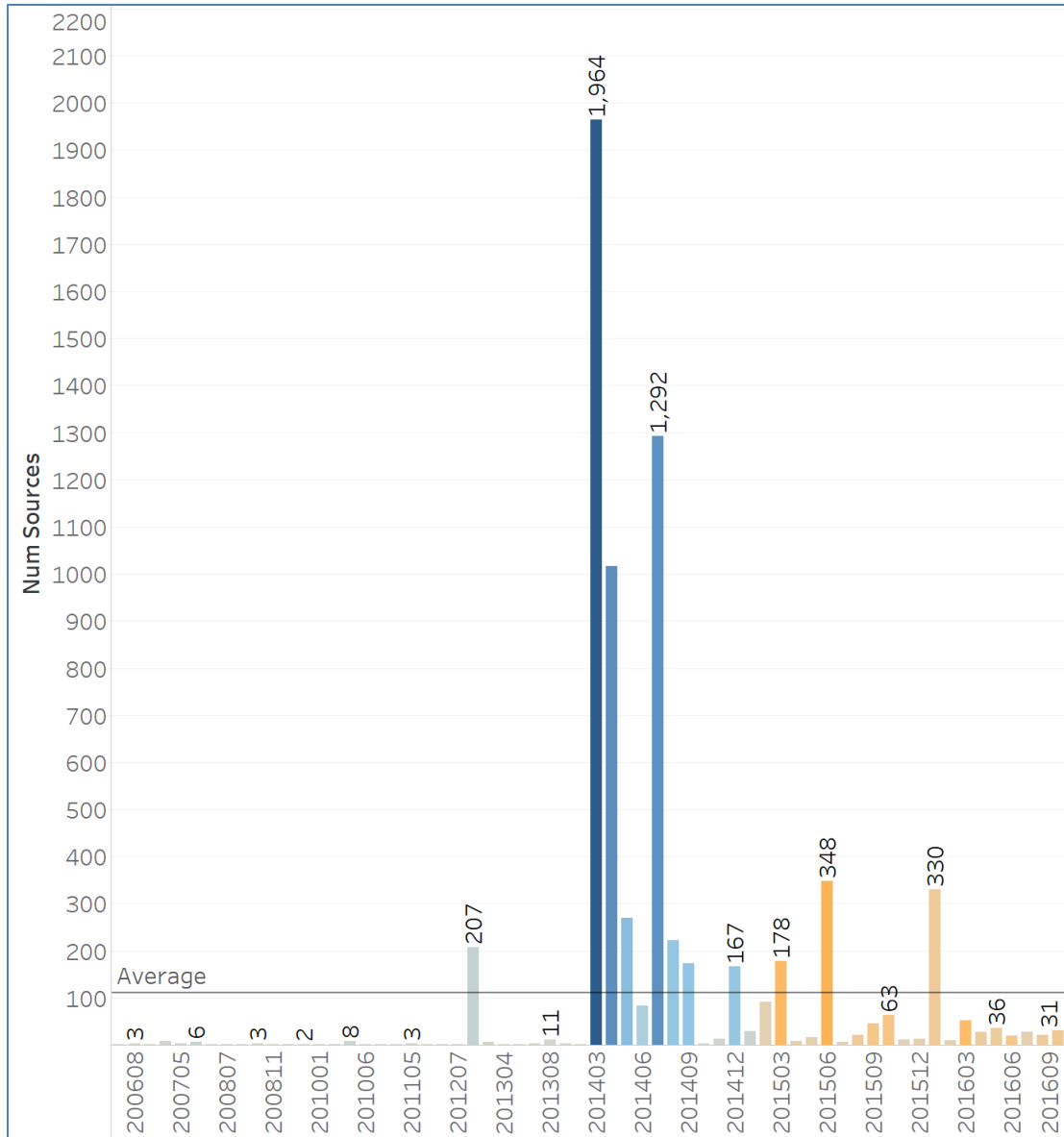


Figure 25: U.S. government economic threats and actions toward Russia, not just the Russian government.

Despite the chart being limited to terms focused on economic tools, rather than general terms like *threat*, we can quickly see the broader definition (*Russia* instead of *Russian government*) was key to revealing a larger number of events. The first thing to jump out from the new timeline, matched by the Russian government sentiment timeline below, is the dramatic jump in positive reporting *by both*

countries in March 2014. The cause(s) of the jump are quite puzzling – March 2014 saw Russia officially annex the Crimea, the U.S. submit a UN Security Council resolution (eventually vetoed by Russia) calling the annexation illegal, the G8 suspend Russia over Crimea, and the U.S. impose economic sanctions on Russia, again in response to the situation in Crimea. Despite all of these negative events, GDELT shows dramatic spikes in reporting and positive sentiment in both countries, with reports on U.S. government activities remaining elevated and positive through the summer of 2014, clearly a time of worsening relations between the U.S. and Russia. Why?

The reason for the jump in sources and reporting is clear – these are important, newsworthy events that would naturally lead to a spike in reporting. As for the dark blue, very positive sentiment, there is no clear answer. Oil prices and the value of the ruble were steady in March 2014. Perhaps negative sentiment dominating the military category caused the economic discussion to turn positive in comparison? The military chart above for March 2014 remains positive, thereby decreasing this possibility. For the Russian side, it is possible the government was attempting to influence foreign governments, including the U.S., with positive rhetoric in order to calm tensions and reduce economic repercussions from the annexation of Crimea. This does not, however, explain the positivity of U.S. government sentiment. Further research, outside the scope of this paper, appears necessary to determine why U.S. government sentiment in the economic category (among others), remained positive during this period of, what is widely believed to be, worsening relations and increasing tensions.

On the negative side, as the timelines illustrate, there is much less overlap. The months with the largest number of sources with negative U.S. government sentiment – here being used as a proxy for economic pressure – are June 2015 and January 2016. A look at Russian government sentiment during those months however shows little effect on sentiment or reporting levels. Likewise, the most negative reporting in Russia is in September 2015 and September 2016, two months with below average U.S. government use of economic tools to pressure the Russian government.

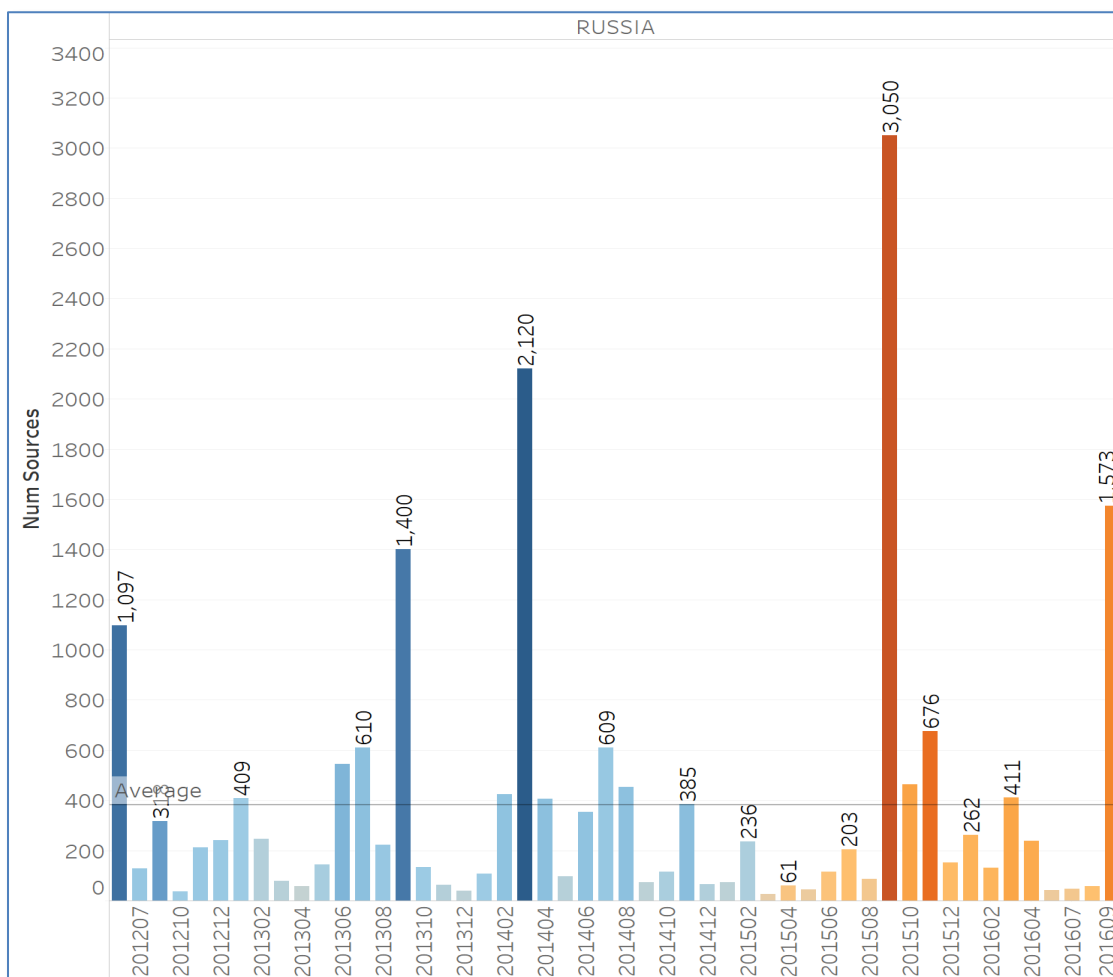


Figure 26: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016.

From this category, we can clearly see a correlation in March 2014 of high levels of reporting and positive sentiment coming from both countries. Though, given Russia's annexation of Crimea that month, with related repercussions for the U.S. – Russia relationship, specifically including economic sanctions, the reason for the positive sentiment is unclear, especially on the part of the U.S. government. More research is needed to unearth the reason(s) for this apparent anomaly.

Aside from the positive reporting and the odd case of March 2014, negative reporting showed little support for the efficacy of using economic tools to threaten or pressure the Russian government. There was no overlap between periods of U.S. pressure and rising negative sentiment in Russia.

Additionally, this section revealed the importance of fully understanding GDELT's ontology – that economic sanctions are coded as not targeting governments – in order to fully explore this category of foreign policy tools. The next category, diplomacy, does not require that change; we can maintain our focus on government-government interaction, again highlighting how GDELT's ontology is far broader and more comprehensive in the military and diplomatic categories than in the economic and information categories.

Diplomacy

As in the categories above, we open our look at the effectiveness of the diplomatic tools of statecraft with a broadly defined categorization timeline. Also as above, only months containing two or more sources are included.

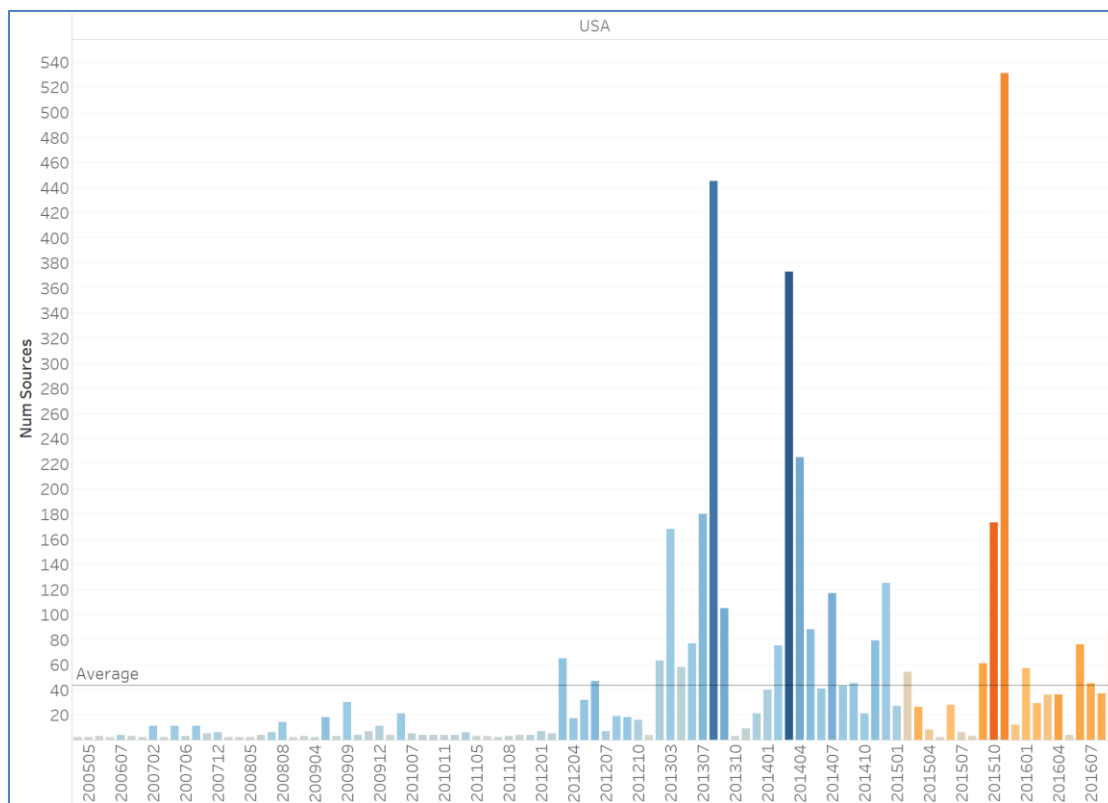


Figure 27: U.S. government diplomatic threats and actions toward the Russian government, broadly categorized.

As before, the early years have far fewer interactions, and are positive or neutral, while later years bring more interaction and, starting in 2015, a permanent switch to negative. The negative turn for U.S. government sentiment in this category starts a couple of months earlier than the previous categories, but otherwise mimics the same pattern of long-term positive sentiment turning negative in early 2015. We will examine the diplomatic interaction in greater detail below, by stripping out much of the overlap with the other categories.

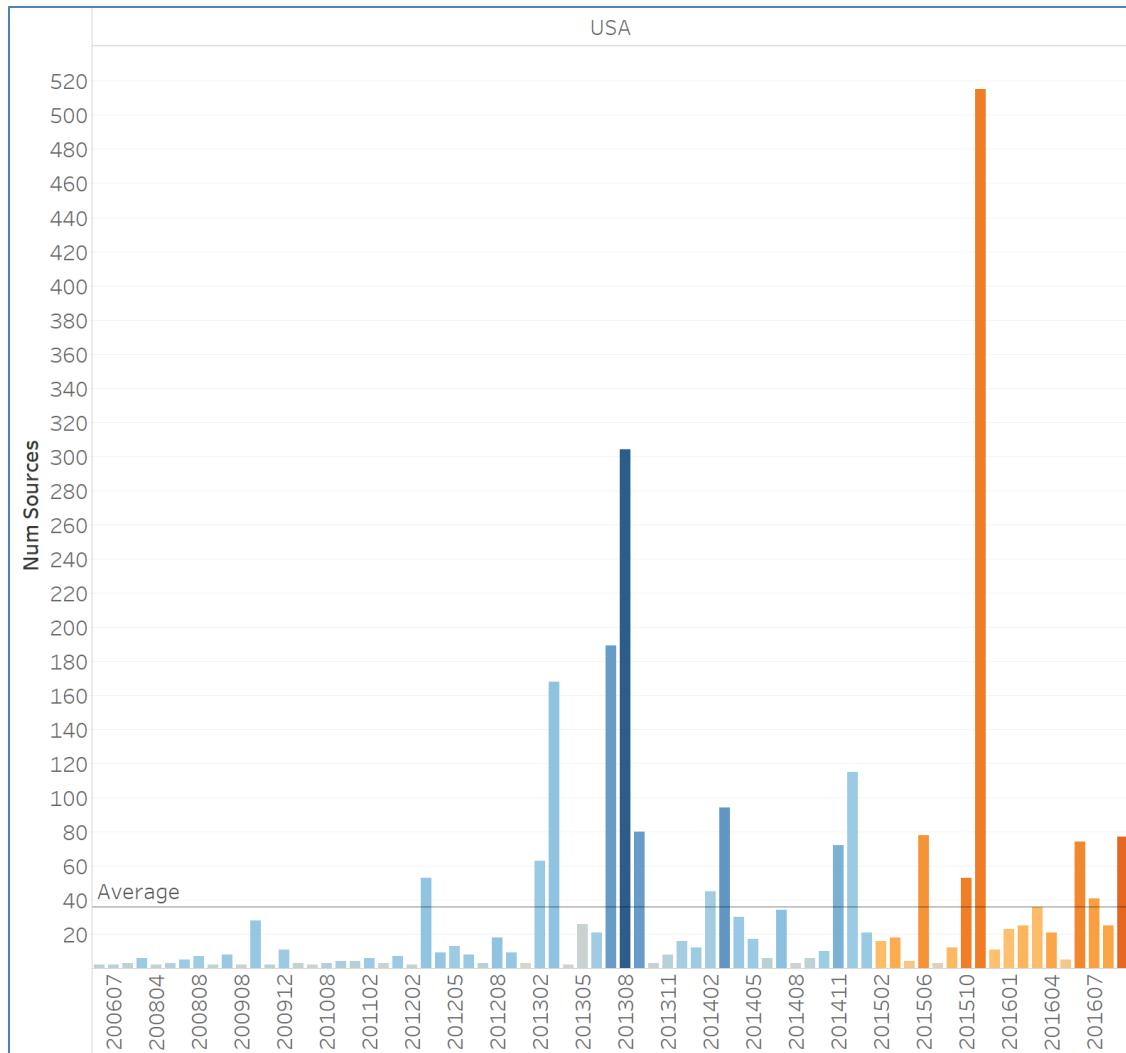


Figure 28: U.S. government diplomatic threats and actions toward the Russian government.

We can quickly see that the larger number of event categories related to diplomacy (like the military) provide a far greater range of data than the economics category, without having to expand GDELT reporting beyond our focus on the Russian government. We can see that the greatest spike in reporting occurs in November 2015, but the chart below reveals little reaction that month from the Russian government. The main event in U.S. – Russia diplomatic relations in

November 2015 was an agreement on Syria reached by Presidents Obama and Putin during a meeting at the G20 summit. It is notable that a month containing an agreement between the two countries generated such an increase in reporting with negative sentiment on the U.S. side, but only a relatively minor increase (also negative) on the Russian side.

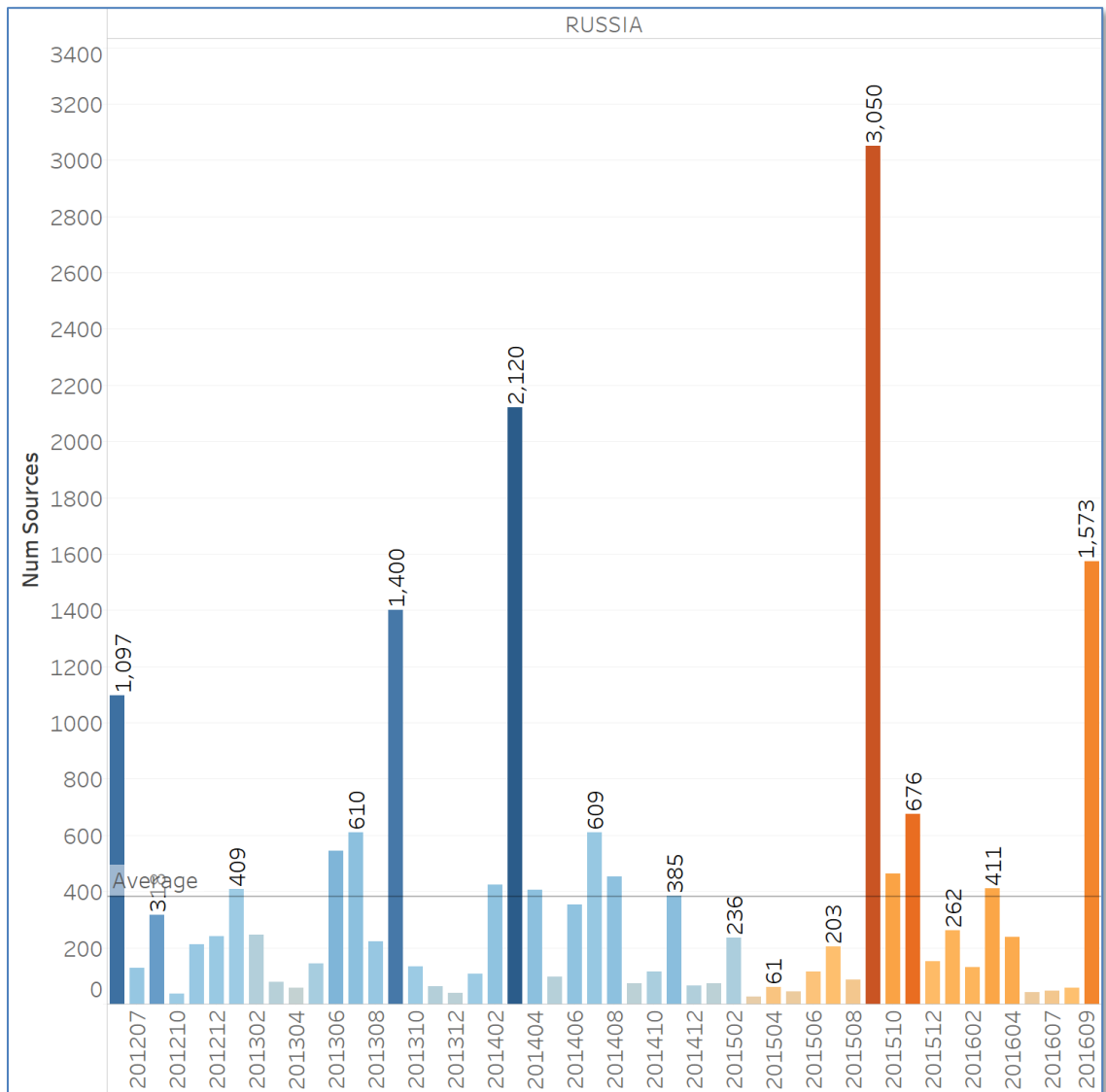


Figure 29: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016.

Likewise, the jump in positive messaging shown in the U.S. timeline for August 2013 generated little reaction from the Russian government. Flipping the examination, months with large spikes in Russian reporting, positive or negative, are not reflected on the U.S. diplomatic timeline. Overall, though sentiment on the two timelines moves roughly in parallel, with similar changes from positive to negative in early 2015, the main peaks in the timelines are not reflective of one-another – meaning we tentatively conclude that U.S. government efforts in the diplomatic category create little effect on the Russian government.

The importance of this finding should not be overlooked. Just as the finding in the information category above, under the TASS and MOFA data, that information could be an effective foreign policy tool, a finding that diplomatic tools do *not* create an effect in the target government has equal or greater policy implications. Especially when paired with the diplomatic category data in the MOFA and TASS section, our data shows U.S. diplomatic efforts toward Russia have been largely ineffectual. Our research focuses on threats (the stick part of the carrots and sticks diptych), so diplomacy may have effectiveness in the positive realm that is hidden here, but so far diplomacy has appeared ineffective as a foreign policy tool.

Information

The information category presents something of a problem when it comes to GDELT. While the military and diplomatic event categories are robust, broad, and well-developed across a diverse array of event types, we saw above that the economic category has far fewer types of specific, unique events. Unfortunately for

our research purposes, the information category is even less developed than the economic category. In part, this is likely a reflection of the traditional unimportance of information as a foreign policy tool, or as a factor in the study of international relations (itself part of the reason for this paper). While the higher politics of diplomacy and the military are well represented in GDELT, the low politics of economics, while not absent, are much less developed. Information appears to have received even less consideration – ‘big data’ imitating, in its own way, traditional preconceptions of what is important in international relations.

This lack of development creates difficulty for our research. There are only a handful of event categories in GDELT that are even tangentially related to information as a tool of foreign policy or international relations. While the image below, of information events broadly categorized, appears to show a well-developed set of event-related data, the much narrower image further below is the key for demonstrating how few information-specific events exist in GDELT.

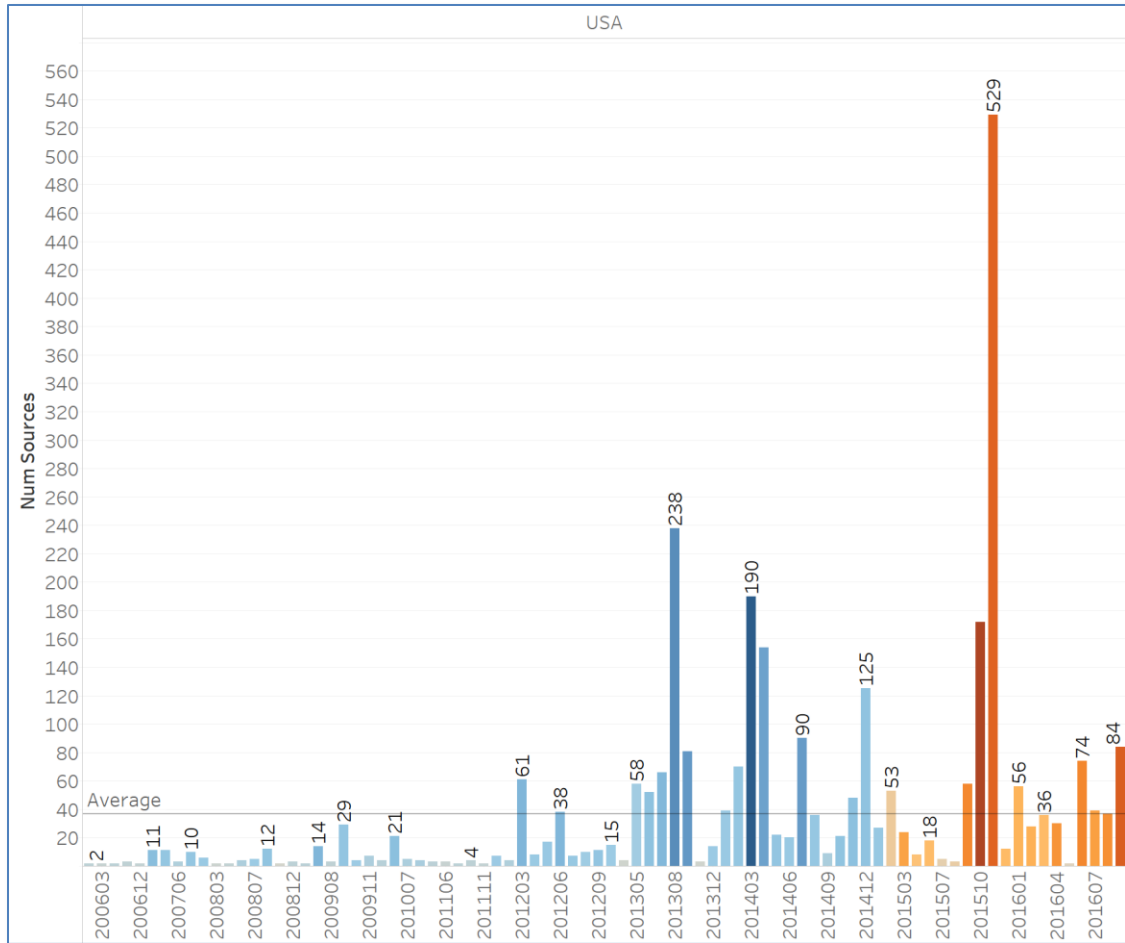


Figure 30: U.S. government information threats and actions toward the Russian government, broadly defined.

Though the image above appears robust, it is largely comprised of false positives – data overlapping from other categories (e.g. the threat category containing the threat of economic sanctions or military action in addition to anything tied to information). The image below brings home the lack of event data for the information category specifically.

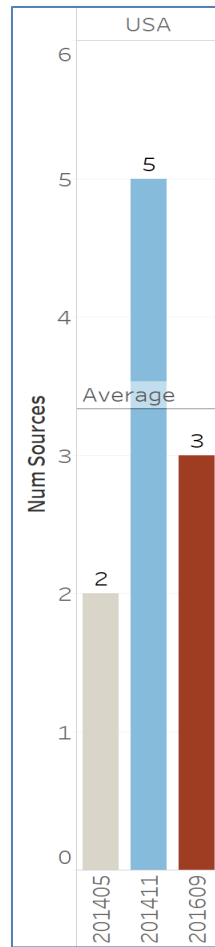


Figure 31: U.S. government information threats and actions toward the Russian government.

Per the image above, we were able to find only three months, all with minimal reporting, with related event data (out of the 10+ years surveyed). Even the categories found, two relating to human rights abuses and one to threats not involving force, are only tangentially related to information and information access. While the economics category had only a few event categories, they were explicitly targeted (e.g. the threat of economic sanctions, the imposition of economic sanctions). This is clearly not the case with the information category.

The timeline below, similar to the expanded one above in the economics category, changes the coding from U.S. government-Russian government, to U.S. government-Russia (all inclusive). This allows for the inclusion of additional event categories, including, for example, the *rally opposition against* code, not available under the previous, more narrow coding. We can see below how these changes result in an increase in events, including several with a robust number of sources.

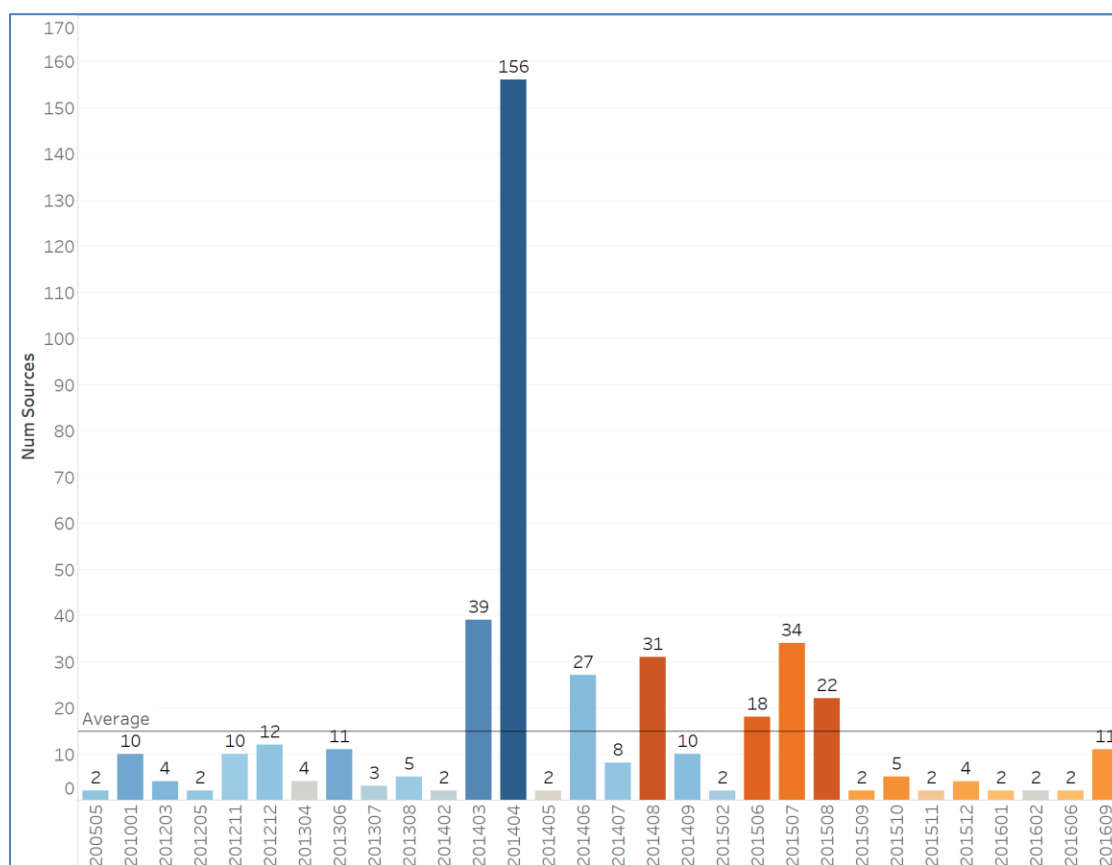


Figure 32: U.S. government information-based threats and actions toward Russia, not just the Russian government.

The timeline of Russian government sentiment below shows that information-based events, what few could be found in the GDELT ontology, did not create much of an impact. The strongly positive U.S. government events in April

2014, per above, created little effect in the Russian government, per below.

Similarly, none of the months with above average negative U.S. government events created an effect in the Russian government. Finally, the months below with the largest number of sources and most negative Russian government sentiment show little correlation with U.S. government efforts in the information category.

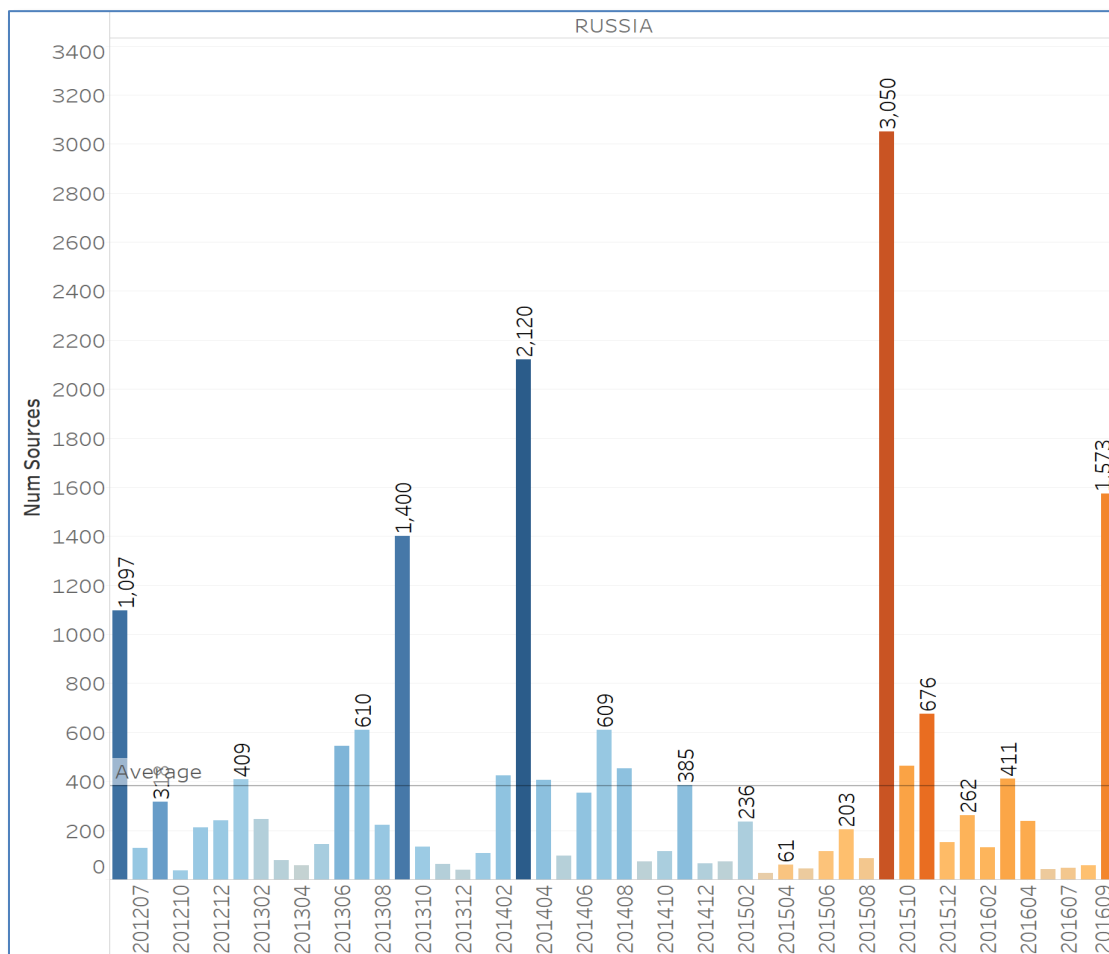


Figure 33: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016.

Unfortunately for our research purposes, there was no connection found between U.S. government use of information as a foreign policy tool and Russian government sentiment or reaction. Additionally, GDELT's lack of information-

related event categories reduces its efficacy for research in the information category. This will likely remain the case not only for Russia, but for the other countries surveyed later in the paper. One possible benefit of this data scarcity is that it further highlights one of the issues raised by the paper, that information is often disregarded as a foreign policy tool. It is important to note that the absence of data clearly does not indicate that information is inefficacious as a foreign policy tool – there is no data to support such a claim! Instead, it highlights the need for such data so the usefulness of information as a foreign policy tool can be addressed.

In an attempt to salvage some additional research efficacy from the GDELT database, we have also developed the timeline below, showing Russian government sentiment, conflict, and actions toward domestic media and the political opposition from 1 January 2005 through September 2016.

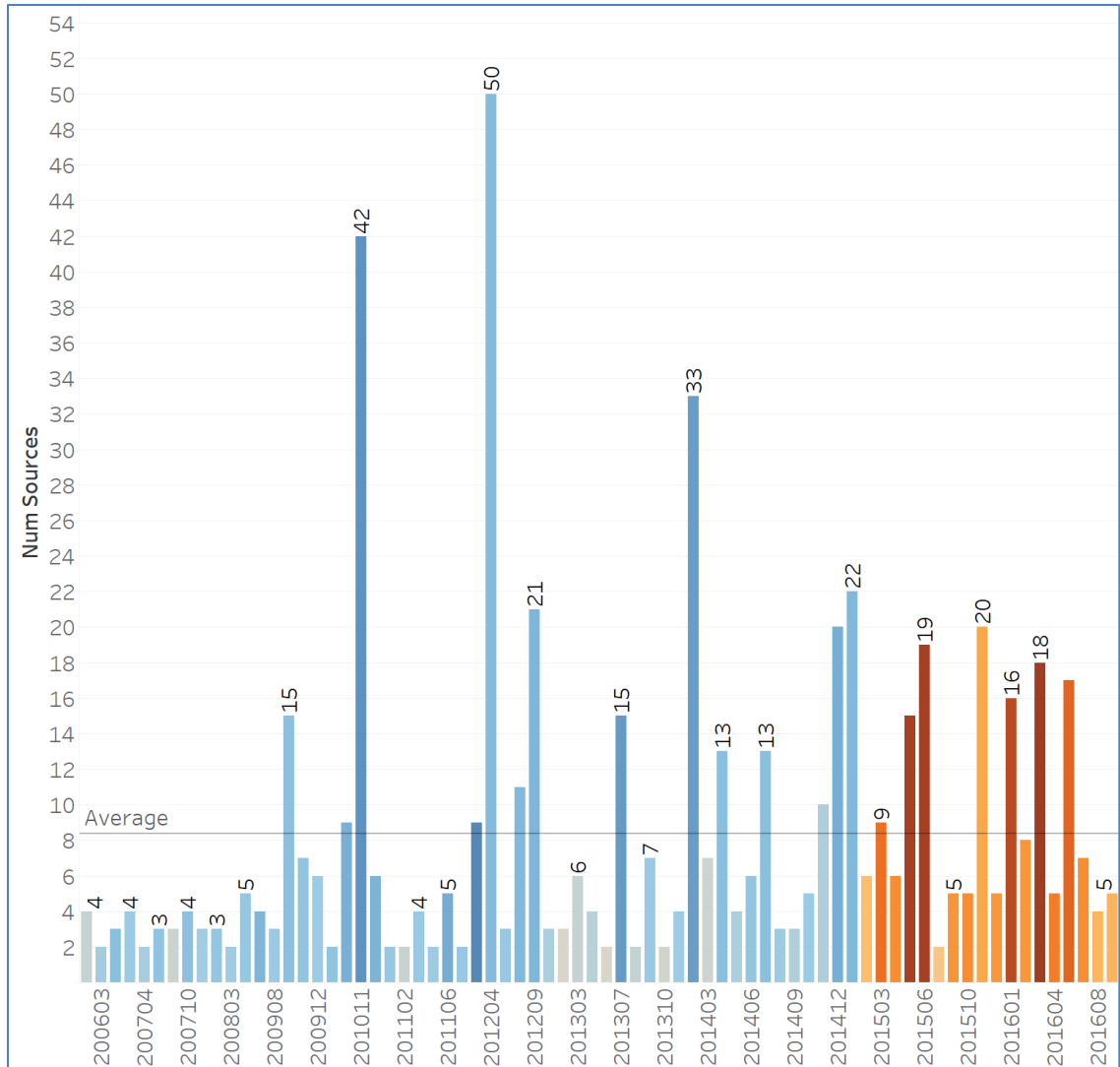


Figure 34: Russian government actions and sentiment toward the Russian media and political opposition.

The first thing to jump out from the timeline is the change in sentiment from late 2014 into early 2015, much like the Russian government's sudden change in sentiment toward the U.S. government. For ease of comparison, we will re-insert that timeline once more, below.

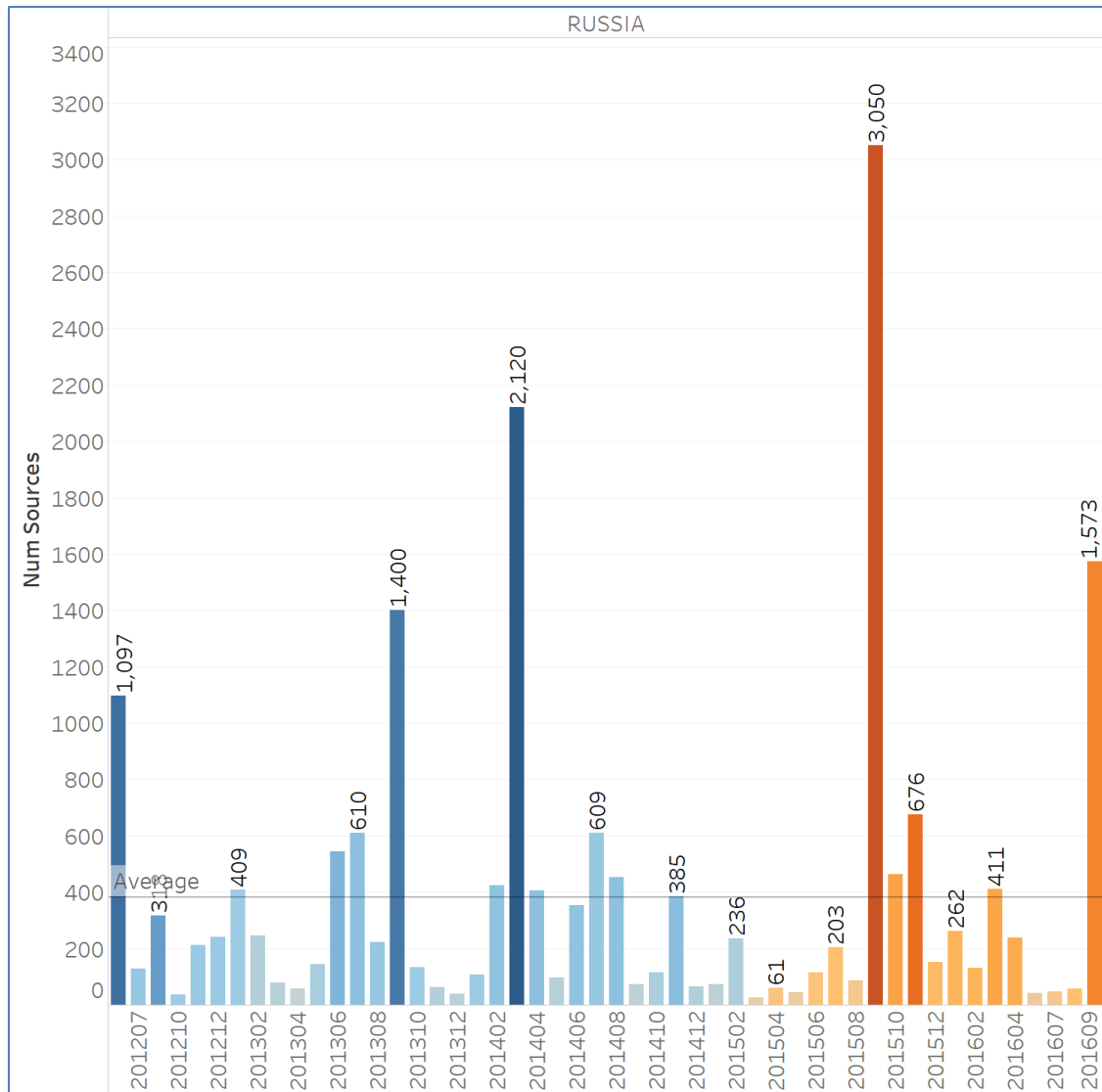


Figure 35: Russian government sentiment toward the U.S. government, June 2012 to Sep. 2016.

From the timelines, we can see that the number of sources are an order of magnitude lower for the internal Russian events than for the international, Russia-U.S. events. Likely this is due to fewer sources carrying stories on internal Russian events than those carrying stories on U.S. – Russia relations, which would include a far greater number of U.S. sources.

While September 2015 represents a clear peak in the timeline on negative Russian government sentiment toward the U.S. government, that same month sees negligible reporting on the media and political opposition timeline. For that timeline, the spikes in sources expressing negative sentiment occur in different months than the international timeline, are much less dramatic, and have a greater number of months near the average.

While the spikes in sources expressing negative sentiment differ in both timelines, what about earlier in the time period, when sentiment was more positive? Here again, the spikes in the numbers of sources do not match. June 2012, September 2013, and March 2014 all see large spikes in the international timeline, but in the domestic timeline those months see no significant deviation. For that timeline, the key months are November 2010, March 2012, and February 2014.

Other than the general trend, of positive sentiment giving way to the negative sentiment starting in 2015, there are few similarities between the two timelines. But what about the other timelines we have seen thus far, is there any possible overlap/relationship between the U.S. government actions and sentiment in the four categories with Russian government relations with domestic media and the political opposition?

For the sake of simplicity and ease of comparison, we re-insert the narrow versions of the timelines from each of the four categories below, followed by the timeline for the Russian government relations with domestic media and the political opposition. We note in advance the information category contains too little data to

draw any meaningful conclusions, but include it for the sake of curiosity and consistency.

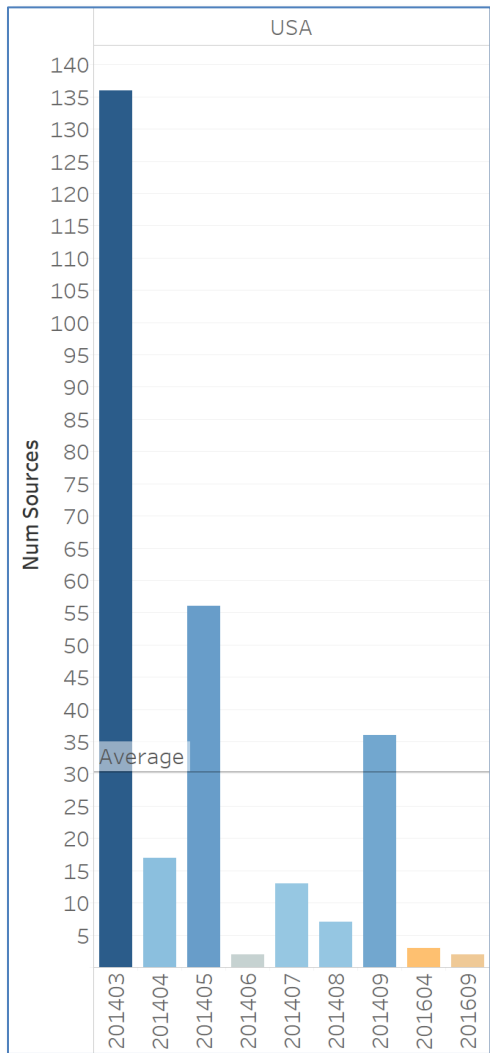


Figure 36: U.S. government economic threats toward the Russian government.

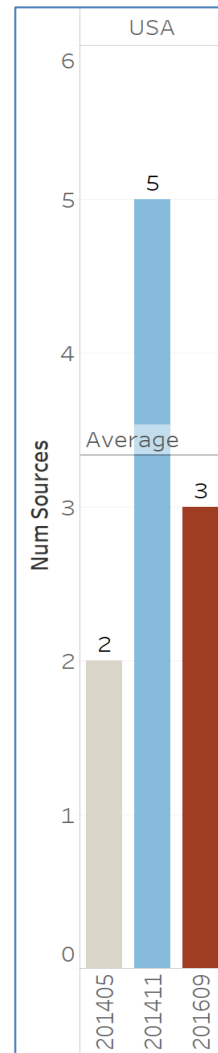


Figure 37: U.S. government information threats toward the Russian government.

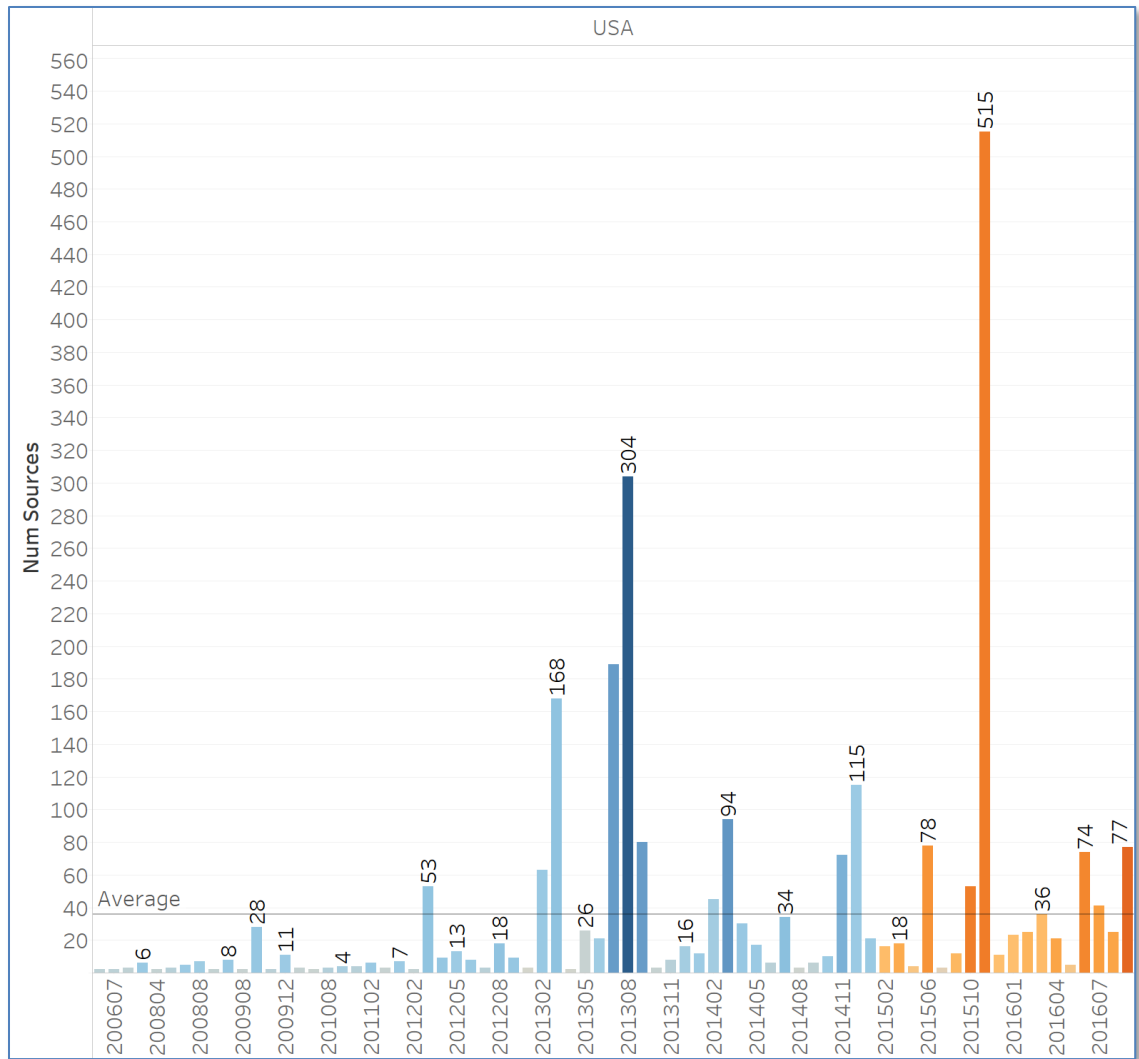


Figure 38: U.S. government diplomatic threats toward the Russian government.

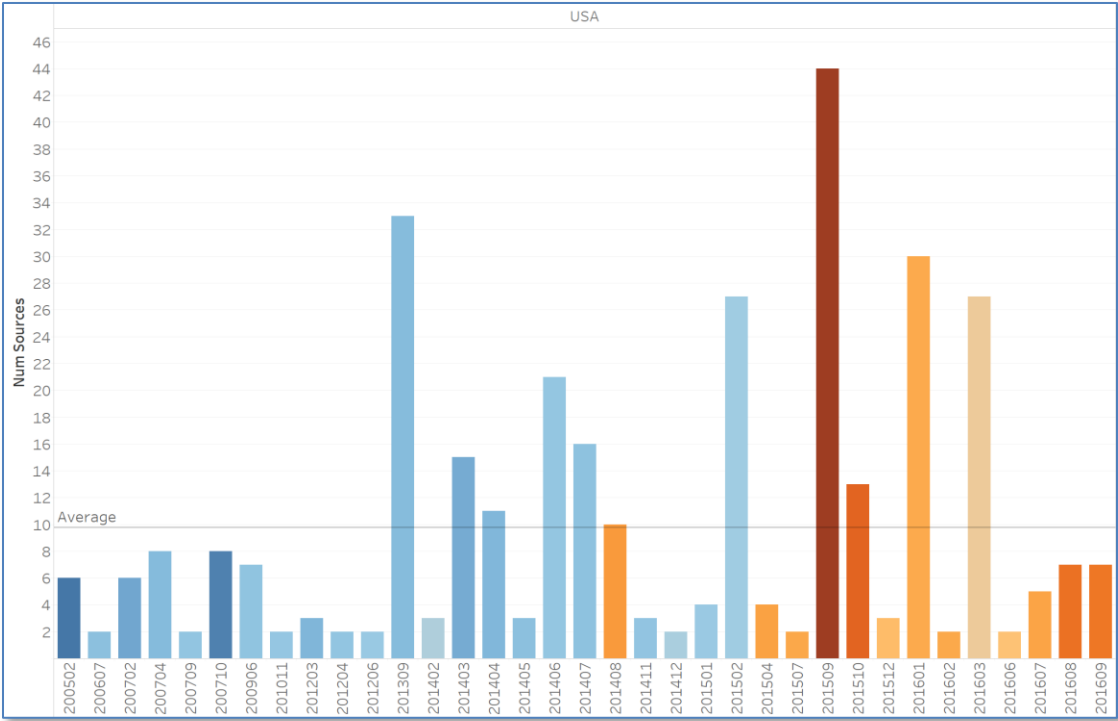


Figure 39: U.S. government military threats toward the Russian government.

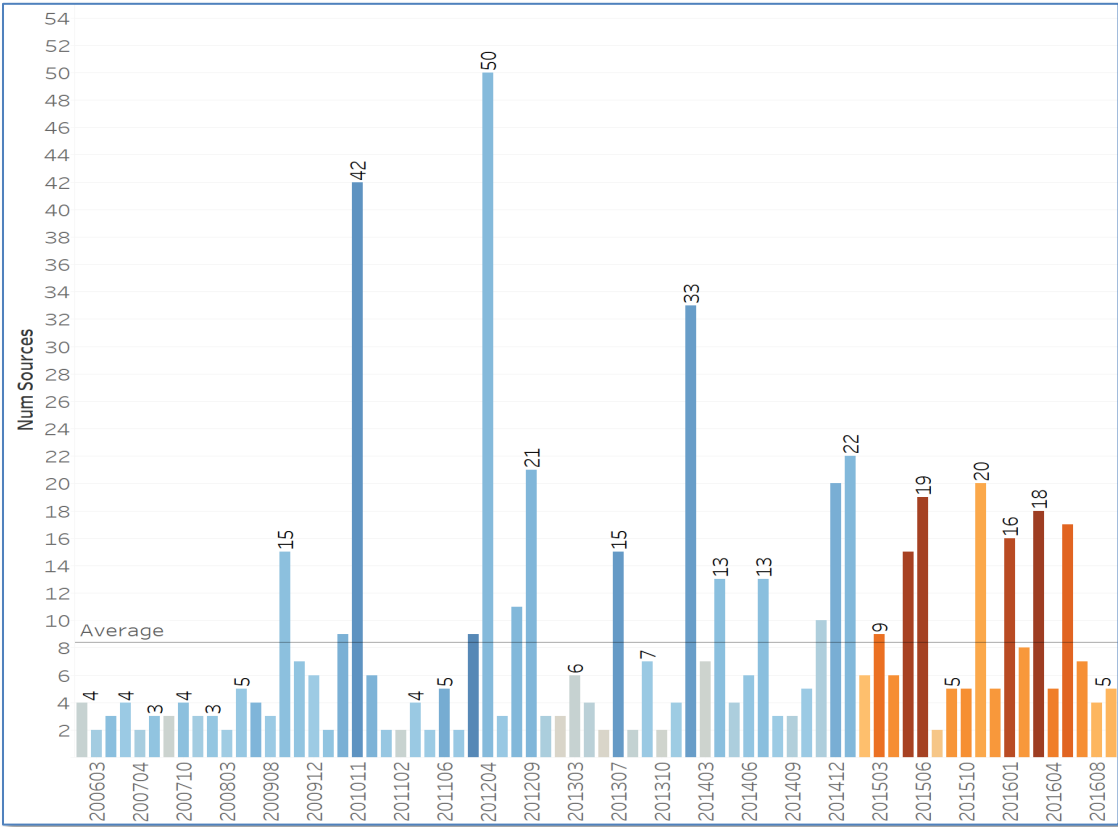


Figure 40: Russian government actions and sentiment toward the Russian media and political opposition.

From the five timelines, we can see the possibility of a correlation between U.S. government diplomatic efforts and Russian government treatment of domestic media and the political opposition, with matching sentiment and spikes in sources in July 2013, December 2014 (both positive), and June and November 2015 (both negative). January and March 2016 also see overlap in the military category between U.S. government efforts and Russian government events targeting domestic media and the political opposition.

These findings are by no means definitive, but do suggest a possible connection between U.S. government efforts targeting the Russian government, and Russian government efforts toward the domestic media and political opposition. A look further above, at the main events examined for the MOFA and TASS reporting, shows no correlation between those events and the Russian government's treatment of domestic media and the political opposition. Together, these findings indicate the possibility that events in the diplomatic and military categories can influence the Russian government's treatment of the political opposition and domestic media. While outside the government-government scope of this paper, this initial finding appears to justify additional, possibly very interesting, research.

GDELT Conclusion

From the GDELT data across the four categories, we can see that the information category contained too little data to be useful, for purposes other than helping to highlight how information is often disregarded as a foreign policy tool.

Even in an information-saturated era of big data, old concepts of foreign policy continue to define the frameworks within which international relations is studied.

Among the other categories, we found that military pressure from the U.S. government initially appeared closely aligned with greater levels of negative Russian government sentiment toward the U.S. government. However, a closer examination revealed an outside issue, Syria, was likely the reason for the apparent correlation. Rather than responding to U.S. activities, the spikes appear to reveal the Russian government's response to U.S. government criticism of its plans and actions in Syria.

In the economic category, we found a crossover between positive economic sentiment by the U.S. government generating positive sentiment from the Russian government, but the reason for this overlap is unclear. The jump in event reporting was ascribed to Russia's invasion of Crimea, but the reason for the high levels of positive sentiment, especially on the part of the U.S. government, is unclear and requires further research. Negative reporting demonstrated even less of a connection, with no overlap between periods of U.S. pressure and rising negative sentiment in Russia.

Finally, in the diplomacy category, we found no possible correlations, positive or negative, between U.S. government events and Russian government sentiment. Similar to the MOFA and TASS reporting examined above, negative diplomatic events appeared to have little impact on Russian government activities or sentiment. As discussed above, this finding is also important, in that it, in effect,

highlights the impotence of U.S. diplomatic efforts targeting the Russian government.

Overall Conclusion

One of the goals of this paper is to determine whether information can be used as a tool of foreign policy on par with more traditional military, diplomatic, and economic tools. In the first section of our research into Russia the research found information was indeed a powerful tool that affected Russian government actions and sentiment. Specifically, pressure from the international press and internet freedom organization Freedom House created a powerfully negative reaction within Russia's government. Separate pressure in the information environment from other organizations, including the U.S. State Department, caused the Russian government to take the interesting step of harnessing the reports to divert attention from Russia's own record and onto the records of countries with which it was in conflict.

Combined, these two reactions demonstrate that activities and tools in the information environment can elicit responses at least as strong as those in the other three categories. Noting the strength and level of negativity of Russian reaction to information tools, the future threat of their use by the U.S. government may be more effective in achieving U.S. aims than the threat or use of tools from one of the other, more traditional, categories.

The second section of the chapter used GDELT data in an attempt to examine Russian government reaction to U.S. government foreign policy tools in the same four categories. The results here were less clear. The information category had

insufficient data to draw any conclusions. The economics category showed a strong correlation, but only on the positive side and only at a time (Russia's invasion of Crimea in March 2014) when reason(s) for positive sentiment are unclear. This possible correlation disappeared on the opposite side, when the U.S. government attempted negative economic measures – during those periods there was no observed overlap between U.S. efforts and Russian reaction.

The diplomatic category had sufficient data, but showed no connection between U.S. government diplomatic efforts and Russian government actions or sentiment. As noted above, this finding supports the idea that U.S. diplomatic efforts toward Russia have been ineffective. A related finding was the possibility that U.S. diplomatic efforts may influence Russian government relations with its political opposition and domestic media – though the finding was tenuous and outside the scope of this paper, it was also the only example of an effect created by U.S. diplomatic efforts toward Russia.

The military category, like the diplomatic category, had large amounts of data in GDELT. This category also showed a possible correlation between U.S. government activities and Russian government reaction, with both experiencing significant spikes in September 2015. However, the event(s) driving the apparent correlation are assessed as related to events in Syria rather than U.S. government efforts to pressure the Russian government (e.g. through NATO exercises in the Baltics).

Overall, the research conducted using GDELT data found little clear correlation between U.S. government use of these foreign policy tools and Russian

government reaction, in any of the four categories. Though possible correlations were found in the military and economic categories, unrelated factors likely influenced the data and induced false positives.

The GDELT data also offered three other findings:

First, across all categories, early 2015 brought a positive to negative shift in *both* governments' sentiment toward the opposite government. This occurred after years of sentiment that had remained positive even during times of strain and crisis. It is unclear why this change occurred, or why it did so in early 2015, but this would appear a fruitful area for future research.

Second, and perhaps providing a clue to the change observed above, in early 2015 Russian government sentiment toward domestic media and the political opposition also turned negative. This also occurred after years of predominantly positive sentiment. Taken together, this finding and the one above may signal a decision to change policy made within the Russian government sometime during the winter of 2014-2015. Since that time, after years of predominantly positive sentiment, Russian government sentiment toward the U.S. government, Russian domestic media, and Russia's political opposition has remained negative.

Third, the research using GDELT data found possible connections between U.S. government activities in the diplomatic and military categories and the Russian government's treatment of its domestic media and political opposition. Establishing a connection between U.S. government policies toward the Russian government and Russia's treatment of its political opposition and domestic media is one of the most intriguing areas for future research suggested by our research.

In closing, this chapter has found a correlation between pressure in the information category and the reaction of the Russian government, both in sentiment (e.g. negative TASS reporting) and activities (i.e. attempting to deflect negative attention onto other states). While this finding is by no means definitive or complete, it does support the premise stated at the outset that information can be productively used as a foreign policy tool. We will conduct additional research to test whether these conclusions hold in more restrictive information environments in the following chapter, on North Korea.

Chapter Five: North Korea

International press and human rights organizations commonly rank North Korea at or near the bottom of rankings measuring freedom of the press and freedom of information. In the *2017 World Press Freedom Index* (<https://rsf.org/en/ranking>) compiled by Reporters Without Borders (<https://rsf.org/>), North Korea ranked last, 180 out of 180 countries surveyed, in terms of its media freedom.¹⁴⁹ In Freedom House's ranking of *Freedom in the World 2017* (<https://freedomhouse.org/report/freedom-world/freedom-world-2017#anchor-one>), North Korea received a three out of a possible score of one hundred (with 100 as most free, 0 as least free), ranking ahead of Syria and Tibet while tying Eritrea and Turkmenistan.¹⁵⁰ ¹⁵¹ North Korea's rank was similar on Freedom House's 2017 ranking of freedom of the press (<https://freedomhouse.org/report/freedom-press/freedom-press-2017>), scoring 98 out of a possible 100 (confusingly, in this report, 0 is most free and 100 is least free), tying Turkmenistan for the lowest ranking in the survey.¹⁵²

This lack of freedom to access information outside that provided by the North Korean state is also commonly noted by regionally-focused scholars and practitioners. Several cite the regime's desire to control the country's information environment as a key factor in the North's governance.

¹⁴⁹ Reporters Without Borders. "2017 World Press Freedom Index."

¹⁵⁰ Freedom House. "Freedom in the World 2017."

¹⁵¹ Puddington and Roylance. "Freedom in the World 2017 - Populists and Autocrats: The Dual Threat to Global Democracy."

¹⁵² Freedom House. "Freedom of the Press 2017: Press Freedom's Dark Horizon."

Victor Cha, Georgetown scholar and former Director for Asian Affairs at the National Security Council during the George W. Bush administration (and, as of December 2017, President Trump's nominee for U.S. Ambassador to South Korea) is among the most explicit. "The DPRK [North Korea] regime is only as strong as its ability to control knowledge. [...] Without control of information, there is no ideology. Without ideology, there is no North Korea as we know it."¹⁵³

Former Soviet exchange student in Pyongyang and current Professor of History at South Korea's Kookmin University, Andrei Lankov, compares North Korean vulnerability to that of the Soviet Union, the former Eastern Europe, and China. Lankov argues that the Soviet Union and communist regimes of Eastern Europe collapsed not due to the sight of "vote counting at an American polling station," but rather to the "sight of [full] shelves at an American supermarket."¹⁵⁴ Similarly, China was forced to begin liberalizing economically in the 1970s because enough decision makers "knew that China was lagging behind and this knowledge prompted them to act."¹⁵⁵ To Lankov, the key to the transformation of these countries was knowledge accumulating over time, most importantly among members of the elite, that people in the West "were living lives that were both more affluent and less controlled by the authorities."¹⁵⁶ Had Soviet authorities, for example, been willing to maintain the level of "isolation and repressiveness"

¹⁵³ Cha, *The Impossible State*, pg. 461.

¹⁵⁴ Lankov, *The Real North Korea*, pgs. 213-214.

¹⁵⁵ *IBID*, pgs 213-215.

¹⁵⁶ *IBID*.

currently maintained by North Korea, “the Soviet Union might still be in existence today.”¹⁵⁷

Compared to these regimes, “If anything, North Korea is even more vulnerable to outside information than the Soviet Union and Eastern European countries used to be.”¹⁵⁸ Lankov continues, “In order to initiate changes in North Korea, it is necessary to put North Korea’s rulers under pressure from its people and the lower echelons of the elite. [...] The only long-term solution, therefore, is to increase internal pressure for a regime transformation, and the major way to achieve this is to increase North Koreans’ awareness of the outside world.”¹⁵⁹

In a separate *Foreign Affairs* essay from 2009, Lankov provides one of the clearest, most concise descriptions available on the North Korean domestic information environment. The report is worth quoting at length:

“North Korean leaders have taken information control to extremes unprecedented even among communist dictatorships. Since the late 1950s, it has been a crime for a North Korean to possess a tunable radio, and all radios sold legally are set only to official broadcasts. In libraries, all nontechnical foreign publications, such as novels and books on politics and history, are placed in special sections accessible only to users with proper security clearance. Private trips overseas are exceptional, even for government officials. North Korea is the world's only country without Internet access for the general public (although there is a small, growing intranet system maintained by the government). These measures seek to ensure that the public believes the official portrayal of North Korea as an island of happiness and

¹⁵⁷ IBID.

¹⁵⁸ IBID, pgs. 214-215.

¹⁵⁹ IBID.

*prosperity in an ocean of suffering. (South Korea suffers "under the yoke of U.S. domination and subjugation, its sovereignty wantonly violated," reports the official North Korean news agency.)"*¹⁶⁰

In the same *Foreign Affairs* article, Lankov also explicitly lays out the failures of previous methods to induce change in North Korea.¹⁶¹ Military coercion is unrealistic; financial sanctions ineffective; expectations that diplomacy, patience, and goodwill can induce reforms are a false hope – instead, the only way to advance the interests of the U.S., South Korea, and their allies is to bring about pressure for change from within North Korea, and the way to do this is through cracking Pyongyang's control over information and introducing truth and information into the North.¹⁶²

B. R. Myers, North Korea specialist, literary critic for *The Atlantic*, and Director of the International Studies Department at South Korea's Dongseo University, takes a slightly different view. To Myers, the key is not extrapolation from Cold War history, nor the infiltration of blue jeans and Hollywood movies. Instead, what is most dangerous to the regime is the spread of public awareness that South Koreans are happy with their international trade, foreign relations, and politico-economic system and do not yearn for rule from their co-ethnics in Pyongyang.¹⁶³ While Lankov and Myers, differ in the details, their underlying messages dovetail: the spread of information contradictory to the regime's

¹⁶⁰ Lankov, Changing North Korea, accessed 16 January 2016.

¹⁶¹ Lankov, Changing North Korea, accessed 16 January 2016.

¹⁶² Ibid, accessed 17 January 2016.

¹⁶³ Myers, 168-169.

propaganda (what Myers deems ‘the Text’), is what most threatens North Korea’s rulers.

U.S. foreign service officer and State Department North Korea specialist Patrick McEachern argues the need for additional coercive tools aside from the “traditional arsenal” of coercive economic measures or UN Security Council resolutions in his 2010 study of the North’s political institutions.¹⁶⁴ His research contends that the “stick” of illicit radios, cell phones, and South Korean dramas is more likely to undermine the regime by impacting the rulers’ claim to legitimacy than economic or financial sanctions.¹⁶⁵ “Information penetration can help instill a wider acceptance of notions that there may be a better future available for the masses and perhaps influence some elites over time to support a more moderate domestic and foreign policy.”¹⁶⁶

Unlike many scholars of the North (aside from Lankov), former British ambassador to North Korea John Everard writes based on years of experience working inside the country. Everard writes evocatively of the “vital” importance to the regime of information control. “The principal form of political control was an attempt to enclose all citizens within a mental world created by the regime. This had two key components – restriction of information about the real world, and the creation through propaganda of an alternative universe of partial truth and downright lies, in which the DPRK appeared to be a near-paradise run by an

¹⁶⁴ McEachern, pg. 233.

¹⁶⁵ McEachern, pg. 233.

¹⁶⁶ McEachern, pg. 233.

omniscient demigod rather than a decrepit and backward state run by crusty old men.”¹⁶⁷

Park Sokeel, director of research and strategy for Liberty in North Korea (LiNK), one of the better-known NGOs that assist North Koreans attempting to escape the North, echoes the information focus, while adding an economic dimension, “We confront North Korea on the territory of Pyongyang’s choosing [when we take the militaristic route] [brackets in original], where they are most comfortable and confident — the military standoff, mutual threat, pressure, isolation and embargo. By focusing so much on traditional security, we play to the regime’s strengths and reinforce their ideologies and siege mentality. It is much cheaper and easier to make progress in the long term if we choose a territory where we are much stronger, namely in the people-centered dimensions of information, culture, and market economics.”¹⁶⁸

Further afield, Robert Litwak, Director of International Security Studies at the Woodrow Wilson International Center and former Director for Nonproliferation on the National Security Council, divides approaches to ‘rogue states’ from Iran to North Korea into *hard landing* and *soft landing* approaches. For Litwak, a key to the soft-landing approach of promoting internal change within the North (rather than the hard landing approach of imposing change from without) is to end the regime’s monopoly on information. Unlike many others quoted here, who speak in more

¹⁶⁷ Everard, pg. 53.

¹⁶⁸ Heintz, *In the Nuclear Standoff, Ordinary North Koreans Disappear*, 2018.

general terms, Litwak specifically mentions the utility of the proliferation of cellphones and the internet to ending this information monopoly.¹⁶⁹

In summary, the author was unable to find a major recent work of political science, modern history, media studies, or area/regional studies on North Korea or northeast Asia that *didn't* discuss the foundational importance of information control to North Korea's rulers. Crucially, while many have stressed the importance of information control to the regime, it appears no one has attempted to measure this importance. For example, how has the regime reacted to previous external attempts to challenge this information control, and how does that reaction, if any, compare to regime reaction(s) to challenges in the military, economic or diplomatic environments? The relative consensus on the lack of media freedom and information access, coupled with the importance of information control to the North Korean regime, provide a useful scenario for testing the saliency of this research.

Research Method

Leadership interviews, population surveys, and other common techniques are problematic when dealing with Pyongyang, as the North rarely provides the requisite access. The author has visited the North and incorporated anecdotal findings from that trip into previous publications, but access to the country for detailed research on the topics examined here is currently considered unobtainable. The lack of direct access to the country, its leaders, elites, populace, and related data

¹⁶⁹ Litwak, pgs. 282 and 288.

forces outside researchers to develop alternate methods when attempting to examine the North.

One approach is to use North Korean refugees/migrants as a way of examining the country, a method employed during the Cold War for research into the Soviet Union, China, and other areas unavailable to outside/Western researchers. By working through a project funded by the Peterson Institute of International Economics and the MacArthur Foundation, Stephen Haggard (University of California San Diego) and Marcus Noland (Peterson Institute for International Economics), were able to examine the North through a survey of North Korean refugees in China and South Korea that first became a paper,¹⁷⁰ then a book.¹⁷¹ Though the research was mainly on economic conditions within the North, the study contained a political communication category related to our research. This category attempted to gauge the level of political dissent inside the North by coding words along an “escalating ladder of dissent” (e.g. *joke* was gauged less serious than *complain*, which in turn was deemed less serious than *organize against*).¹⁷² By assigning an increasing point value to the terms, from joking about the regime, to complaining about it, to organizing against it, the authors were able to analyze defector sentiment to develop conclusions about political beliefs and information control inside the country.¹⁷³ Of importance for this paper, Haggard and Noland found “evidence that access to [foreign] information is correlated with political

¹⁷⁰ Haggard and Noland, *Political Attitudes under Repression – Evidence from North Korean Refugees*.

¹⁷¹ Haggard and Noland, *Witness to Transformation: Refugee Insights into North Korea*.

¹⁷² Haggard and Noland, *Witness to Transformation: Refugee Insights into North Korea*, pgs. 109-117.

¹⁷³ Haggard and Noland, *Witness to Transformation: Refugee Insights into North Korea*, pgs. 110-111.

attitudes. Consumption of foreign media was associated with more negative assessments of the regime and its intentions.”¹⁷⁴

Of course, as pointed out by critics of using defector testimony as well as the authors themselves, this research has difficulty establishing causation. The defectors are clearly a self-selected group willing to risk punishment for themselves and their families (under Northern law it is illegal to change residence or leave the country without government permission and entire families can be punished for the violations of one member). Are the refugees therefore more likely than others to seek out foreign media/information? Express dissatisfaction with the regime? Engage in dissent? The authors attempt to control for this issue (e.g. timelines to see which came first, access to outside information or a desire to defect), but criticism remains due to concerns over selection bias and sample size.

This paper does not use defector testimony, but does use sentiment analysis as a way of developing a quantitative value to measure the strength of a response. In the case of Haggard and Noland, the research used refugee testimony to gauge public opinion and political freedoms inside the North. In this research, the focus will be on examining official state media to gauge response levels by Pyongyang to outside stimuli attempting to pressure the regime. Per above, these stimuli are classified into four areas: the diplomatic, informational, military, and economic (DIME) tools of statecraft.

As in the chapter on Russia, this chapter examines North Korean government sentiment and actions in response to the four DIME foreign policy tools. By the end

¹⁷⁴ Haggard and Noland, *Witness to Transformation: Refugee Insights into North Korea*, pg. 112.

of the chapter, we intend to provide a clearer idea of which tools produce the strongest negative reactions in the North Korean government. The chapter will close with policy recommendations and suggested areas for future research.

Sources

For our research into North Korea, we used five sources or types of sources:

1. *The Korean Central News Agency* (KCNA – <http://www.kcna.kp>), North Korea's official government news organization
2. *The Rodong Sinmun*, the official media outlet of the ruling Workers'/Labor Party, <http://www.rodong.rep.kp>.
3. *Uriminzokkiri* (roughly, 'Our People's Path', <http://www.uriminzokkiri.com>), a Pyongyang-controlled media outlet that often combines its own reporting with that of the KCNA and the Rodong Sinmun
4. Twitter data from related North Korean accounts
5. Databases: in order to examine North Korean actions (essentially, what the North *did* in addition to what the North officially *said*), this chapter will use databases of related UN resolutions (which include both diplomatic and economic actions);¹⁷⁵ ¹⁷⁶ databases of military exercises, missile launches, and related activities;¹⁷⁷ ¹⁷⁸ and a database of select

¹⁷⁵ Davenport, Kelsey. "UN Security Council Resolutions on North Korea."

¹⁷⁶ Security Council Report. "UN Documents for DPRK (North Korea)."

¹⁷⁷ CSIS. "Beyond Parallel." Washington, DC: Center for Strategic and International Studies.

¹⁷⁸ Center for Nonproliferation Studies. "The CNS North Korea Missile Test Database."

North Korean diplomatic activities and state-level negotiations¹⁷⁹

Before continuing, it is necessary to provide a word of caution regarding official North Korean sources. As mentioned previously, changes in North Korea's power structure or ideological focus can result in alterations or outright culling of previously published media reports. Lacking access to an unfiltered database of North Korean state media reporting, we note here at the outset that this culling may have reduced the amount of data available for our research. The paper will attempt to control for this potential problem through the use of North Korean *actions* in response to outside foreign policy tools. Actions reported by outside sources cannot be culled or altered after the fact by the North in the same way as domestic media reports, providing a clearer, possibly less adulterated view of North Korean responses to the four tools under examination.

Data Collection

Data from the official North Korean websites (*KCNA*, *Rodong Sinmun*, and *Uriminzokkiri*) were collected in August 2017. There were difficulties accessing some of the sites, due to geographic restrictions placed on the websites that attempted to limit access to only certain countries (e.g. access was available from inside Japan, but not from the U.S.). This required the use of a VPN to access the sites from Rutgers and/or New Jersey, where the bulk of this research occurred (VPN:

¹⁷⁹ CSIS. "Beyond Parallel." Washington, DC: Center for Strategic and International Studies.

virtual private network; in this case, one capable of making the user/researcher appear to be accessing the North's websites from inside Japan).

Data were collected from Rodong Sinmun and Uriminzokkiri through searches using specific terms (e.g. the names and numbers of specific UN resolutions, the names and years of U.S. and South Korean military exercises, etc.). Some of the search results were limited, either by the nature of the search (e.g. UN resolutions were normally only mentioned by the media during the time periods they were drafted, debated, and voted on), or by website restrictions/limitations (e.g. the site only maintained two years of records). Search results ranged from fewer than 10 related stories, to several dozen stories. Further details are below, in the corresponding diplomatic, information, military, and economic sections.

By hiring a specialist data collection firm (ScrapingHub, <https://scrapinghub.com/>) to access stories on the KCNA website, the researcher was able to obtain a database of all KCNA reporting in English from January 2002 until August 2017 – a total of just over 100,000 stories. Aside from the research here, this large database of KCNA reporting in English may prove a valuable tool for other researchers on North Korea and will be made available to the community (e.g. through <http://koreanstudies.com>) upon completion of this paper.

For the event databases on North Korean (re)actions, the research primarily uses the Center for Strategic and International Studies' (CSIS) *Beyond Parallel* databases and the Security Council Report's data on UN resolutions targeting North

Korea.^{180 181} The timing of these events also helped drive our searches in North Korean media and provided the key data on North Korean actions possibly correlated with external foreign policy tools targeting the North. Further details are examined in the appropriate sections below.

Korean Central News Agency (KCNA), Rodong Sinmun, Uriminzokkiri

Rodong Sinmun

The first set of articles examined is from the Rodong Sinmun, the official media outlet of North Korea's ruling Worker's Party. *Rodong* can be translated into English as *work* or *labor*; *sinmun* is normally translated as *newspaper* and, just as the English term has come to encompass the online as well as print arms of a newspaper, *sinmun* has come to include the same in Korean. In this paper, Rodong Sinmun (as well as KCNA and Uriminzokkiri), refers to the broadest, print and online, form of the organization.

For the Rodong Sinmun, articles were searched and downloaded in August 2017, with dates available during our searches from January 2016 to August 2017. Anecdotally, North Korea is widely believed to respond most strongly and negatively to joint South Korean and U.S. military exercises held in South Korea, so we will examine military first, followed by economic, diplomatic, and information tools.

¹⁸⁰ CSIS. "Beyond Parallel." Washington, DC: Center for Strategic and International Studies.

¹⁸¹ Security Council Report. "UN Documents for DPRK (North Korea)."

Rodong Sinmun – Military

For the Rodong Sinmun, during the period indicated, we used three search terms: *military exercise*, *foal*, and *ulji*. This captured reporting and sentiment on military exercises in general, plus the specific (and separately held) joint South Korean and U.S. Foal Eagle and Ulji Freedom Guardian (also known as Ulji Focus Lens) military exercises/drills. It is important to note here that when transliterating from the Korean, Pyongyang uses a *J*, and gets Ulji, whereas in the South (including in U.S. references to the exercises) Seoul uses a CH and gets *Ulchi*. Therefore, a researcher looking at the exercises in English is more likely to get results from either the northern or southern side of the DMZ, depending on their spelling of Ulji/Ulchi. Since the focus here is Pyongyang, this research uses the North's spelling.

Of the three search terms (*military exercise*, *ulji*, and *foal*), the specific exercise terms generated the most negative sentiment (61% and 60% negative), with *military exercise* registering slightly lower negative sentiment, at 54%. The details are illustrated below, in order of most to least negative. As a reminder, N+ is very negative, N is negative, NEU is neutral, P is positive, and P+ is very positive.

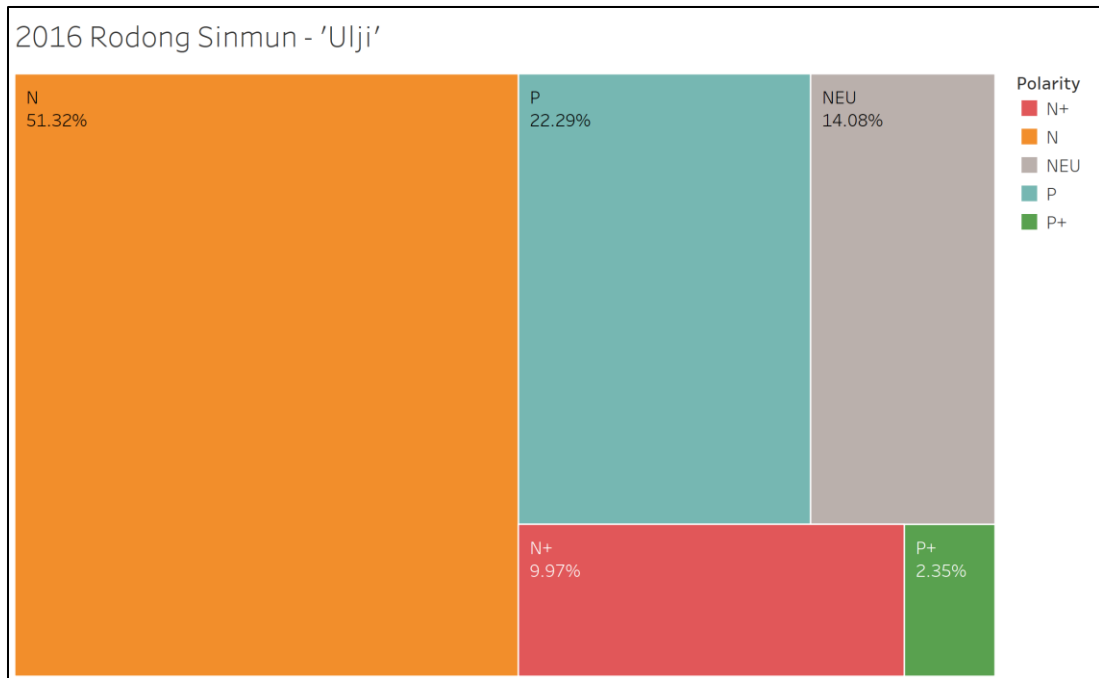


Figure 41: Rodong Sinmun - 'Ulji'

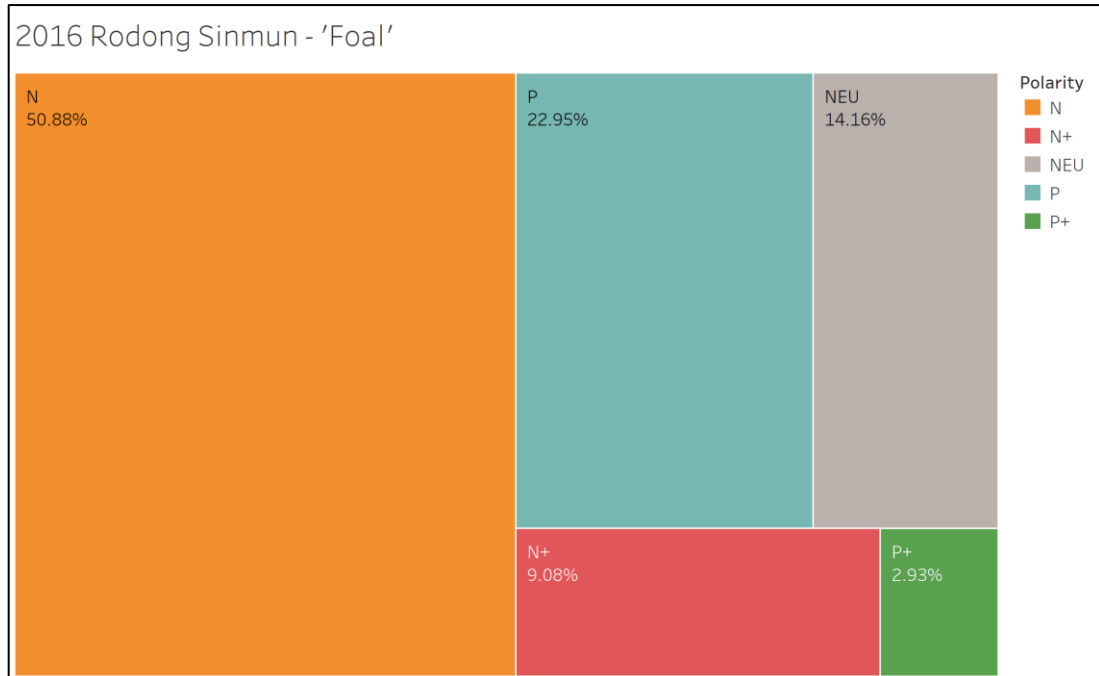


Figure 42: Rodong Sinmun - 'Foal'

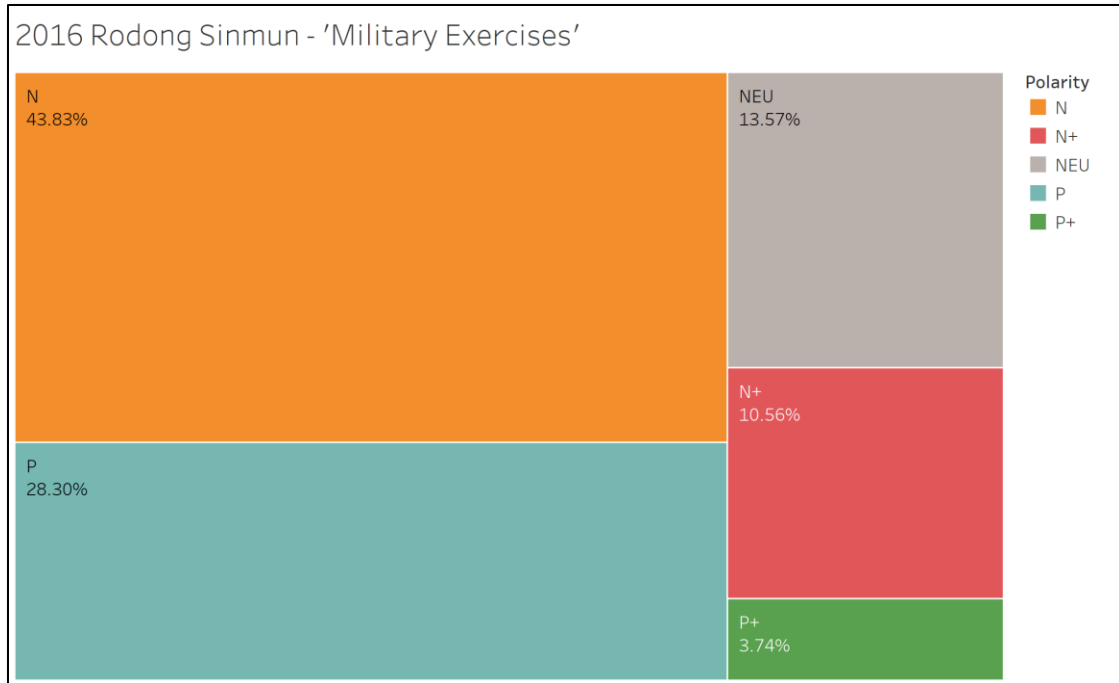


Figure 43: Rodong Sinmun – 'Military Exercises'

Economic

For this tool, the term *sanction* (which includes *sanctions*) was used. The returns cover stories from January to December 2016 and produced notably less negative sentiment, at 46%, than any of the military-related terms, as shown below.

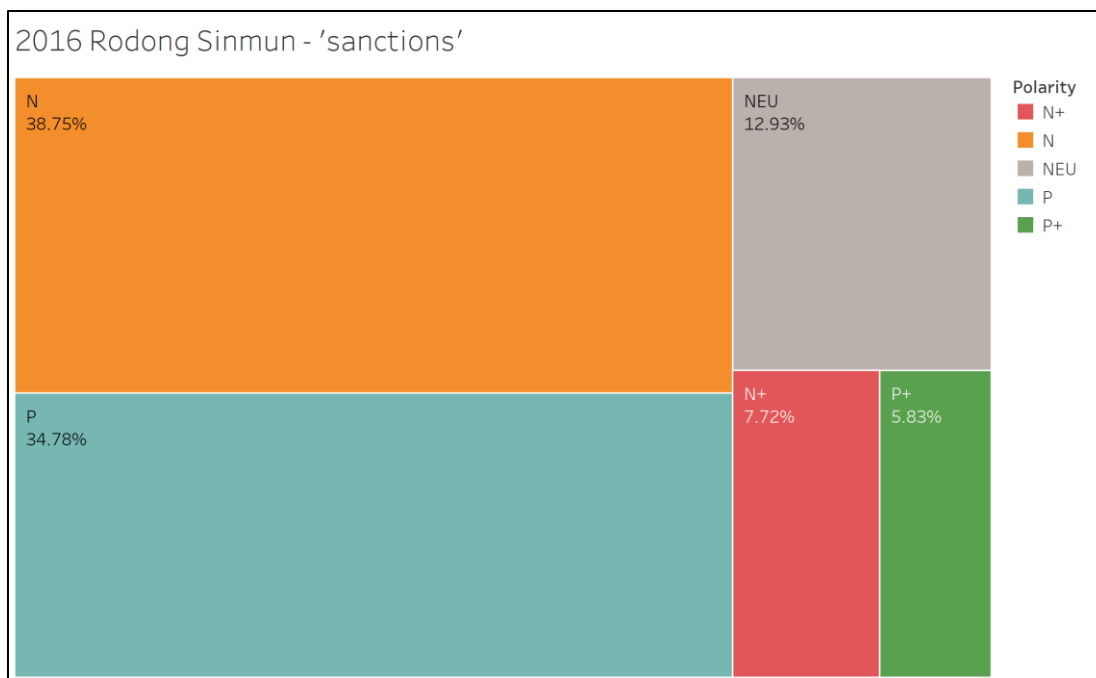


Figure 44: Rodong Sinmun – 'sanctions'

Diplomatic

Most UN resolutions targeting the North also involve economic sanctions, presenting a disaggregation problem – is Pyongyang reacting to diplomatic pressure, economic pressure, or some combination of both? If both, to what respective levels? We will attempt to focus solely on diplomacy in the data from the KCNA, but for the time period surveyed for the Rodong Sinmun, the main UN resolution (#2270 from March 2016) contained elements that condemned the North, as well as expanded existing economic sanctions on the North and thus involves both the diplomatic and economic tools of statecraft (as do many of the other UN resolutions focused on the North). Interestingly, despite this combination of two tools of statecraft, UN Resolution 2270, at 50%, generated only slightly more

negative Rodong Sinmun sentiment than the solely sanctions-focused data examined above.

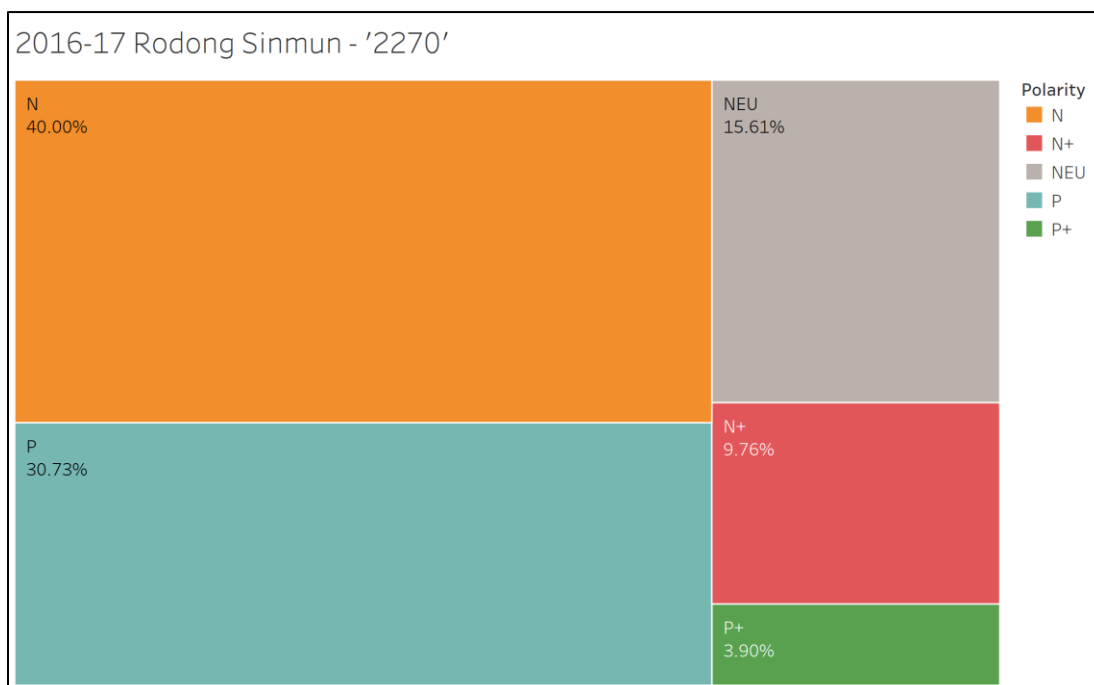


Figure 45: Rodong Sinmun - '2270'

Information

Here we used the terms *psychological warfare* and *loudspeaker(s)* in our searches, with reporting from January 2016 to August 2017. *Psychological warfare* was chosen because it is a term commonly used by the North when discussing the outside (usually South Korea or the U.S.) use of information (e.g. leaflets, loudspeakers) to target its citizens. *Loudspeaker* was chosen because Seoul used loudspeakers during the period surveyed to broadcast information across the border and into the North. While a case can be made that psychological warfare could/should be included in the military section, given the operationalization of the activities (leaflets and loudspeakers) involve primarily information, we have chosen

to include the results here. Of the two terms, psychological warfare was 55% negative, less negative than the specific, named military exercises above, but more negative than *military exercise* and the economic and diplomatic terms. Most interestingly, the term loudspeaker, at 66% negative, generated the most negative sentiment of any term surveyed.

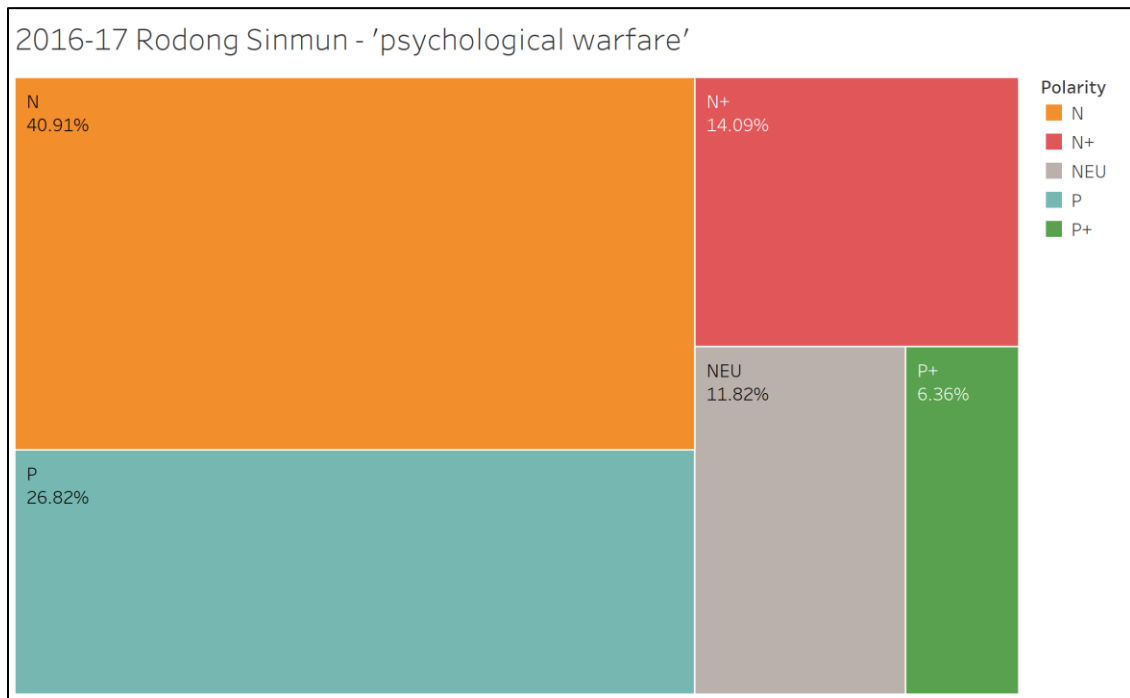


Figure 46: Rodong Sinmun – 'psychological warfare'

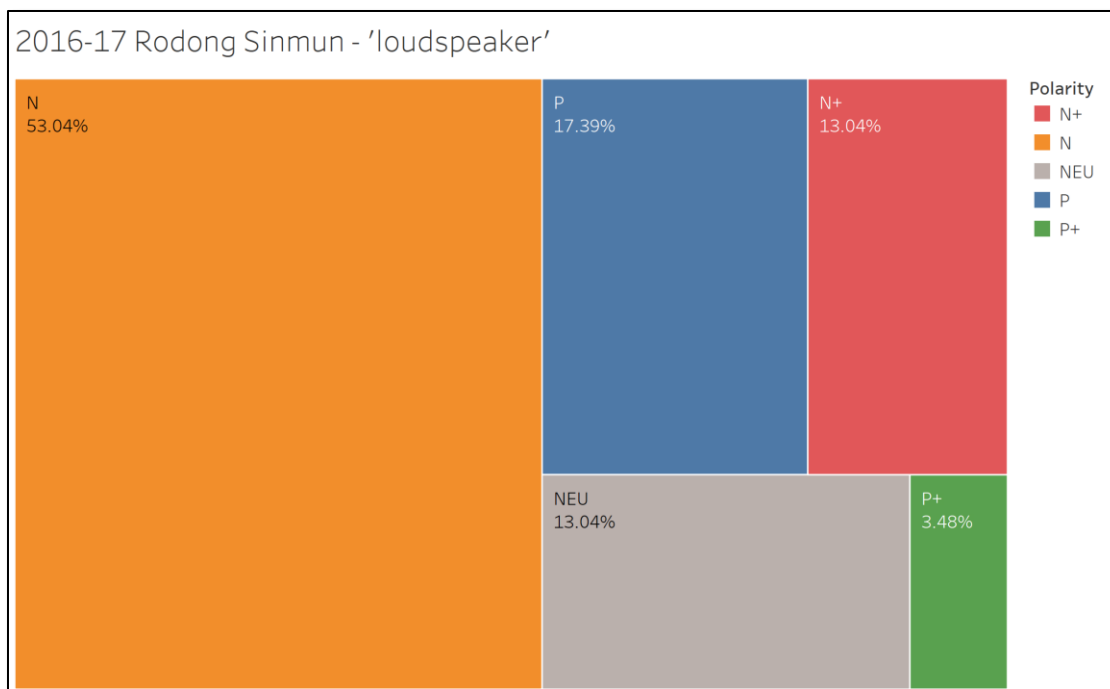


Figure 47: Rodong Sinmun - 'loudspeaker'

In summary, as expected, the military related terms were more negative than the economic and diplomatic terms, but the most negative was the one solely associated with information: *loudspeaker*. These findings support the idea that authoritarian regimes, including North Korea, react quite negatively to pressure in the information environment. This finding also supports the saliency of using information as a tool of foreign policy when dealing with authoritarian states.

Uriminzokkiri

For Uriminzokkiri reporting an additional caveat is in order. While this site generates its own content, it also commonly aggregates content from other North Korean media outlets, commonly including the other two organizations examined

here: Rodong Sinmun and the KCNA. This may lead to some overlap of stories being reported both here and in one of the other sources. Given the focus in this section is on percentage of sentiment rather than total numbers of reports, double-counting is unlikely to affect any findings.

For Uriminzokkiri, the reporting database includes *all* stories from February 2015 until August 2017 – at least, all of the stories that were available in August 2017 when the data was extracted from the site. Collecting all of the stories available on the site, not just the ones relevant to the research, provides a sentiment baseline for Uriminzokkiri reporting, shown below.

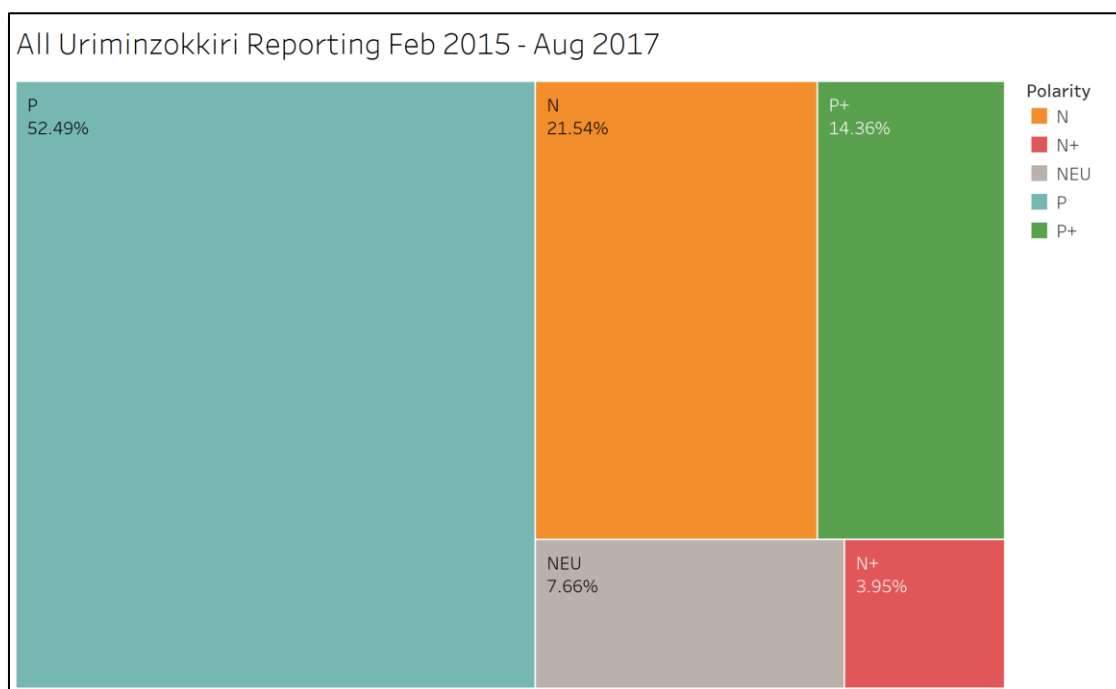


Figure 48: All Uriminzokkiri Reporting Feb 2015 – Aug 2017

From this we can see that overall, Uriminzokkiri reporting is normally much more positive (67%) than negative (25%). In the four upcoming sections, the

baseline sentiment found here is compared with the more targeted findings from the four DIME categories. As above, with the Rodong Sinmun reporting, first is the military category, followed by the economic, diplomatic, and information categories.

Military

The Uriminzokkiri reporting provides an interesting contrast between overall sentiment toward military exercises and the specific sentiment toward the actual joint South Korean and U.S. exercises. First is sentiment toward military exercises in general.

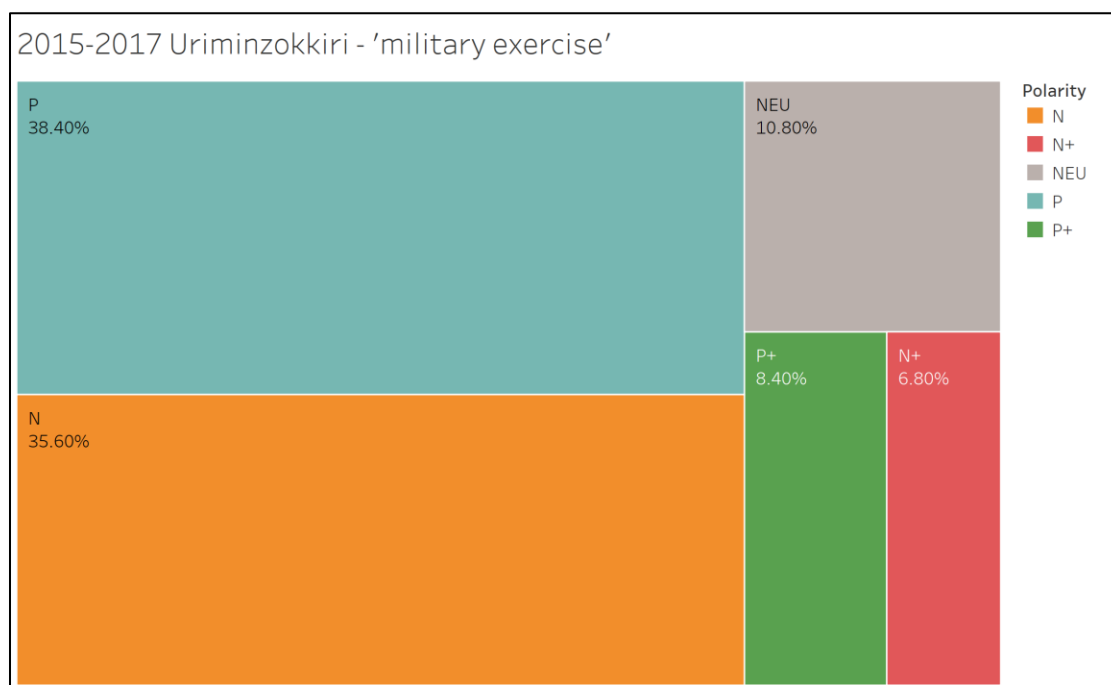


Figure 49: 2015-2017 Uriminzokkiri - 'military exercise'

Here we can see 47% *positive* reporting to 42% negative reporting – a sizeable difference from Rodong Sinmun (54% negative) and a finding not in line

with expectations of how Pyongyang would react to joint military exercises by two countries with which it is still technically at war (the ‘Korean War’ ended in 1953 with a ceasefire and armistice; a peace treaty has never been signed, leaving the belligerents in a state of war).

The other two search terms, *ulji* and *foal*, representing the names of specific joint South Korean and U.S. military exercises, are however, much more in line with both expectations and what was observed in the Rodong Sinmun reporting. One caveat, the findings on the Ulji Focus Lens exercises (‘ulji’) are based on only three stories.

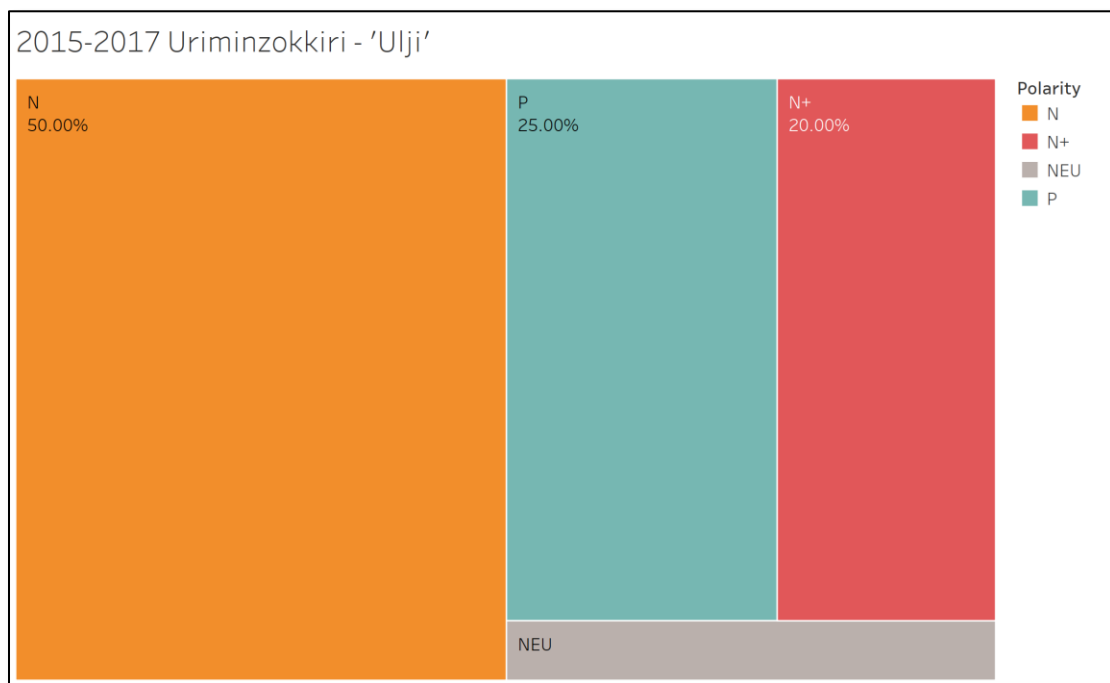


Figure 50: 2015-2017 Uriminzokkiri – ‘Ulji’

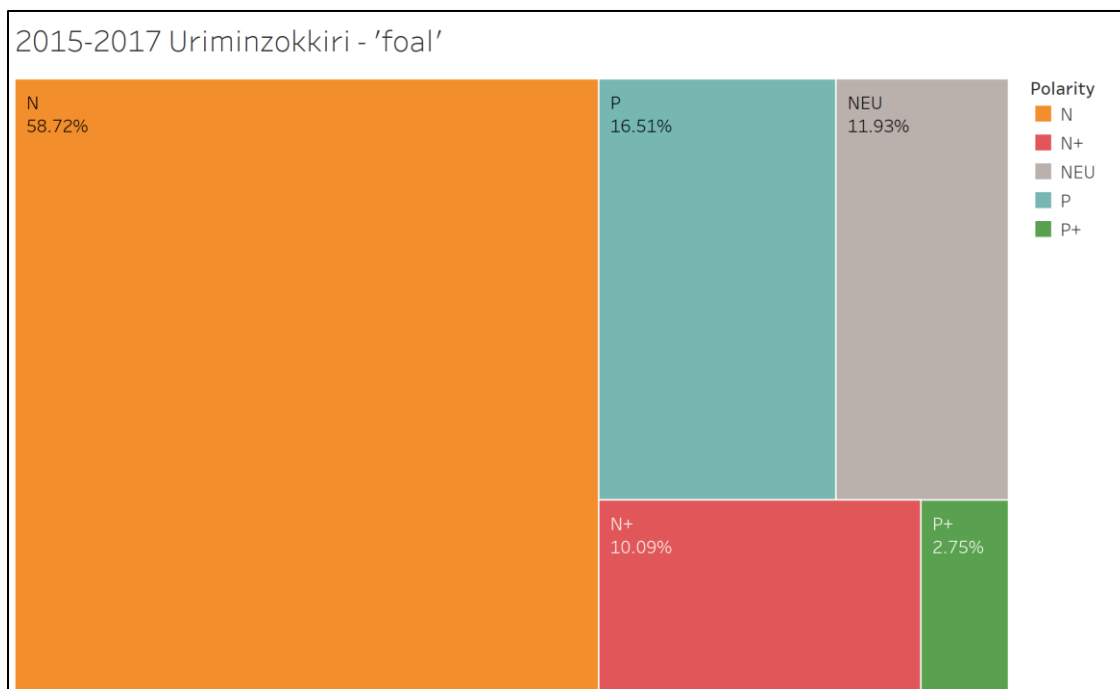


Figure 51: 2015-2017 Uriminzokkiri - 'foal'

The findings here, at 69% and 70% negative, including a rare 20% very negative for ulji, are much more negative than 'military exercise' and approximately 10% more negative than for similar terms in the Rodong Sinmun reporting. This finding is more in line with what many observers of the North, in addition to realist theory, would predict. Also note the contrast of all three search terms with the overall 67% positive reporting noted in the baseline survey discussed above.

Economic

For this tool, like in the Rodong Sinmun reporting above, the term *sanction* (which includes *sanctions*) was used. The returns cover stories from January 2015 to August 2017, approximately 32 months (though not all months had related stories)

compared to 12 months for the Rodong Sinmun data. Interestingly, compared to that found above, this category produced 59% negative sentiment, considerably higher than that for *military exercise*, but lower than for the specific named exercise searches.

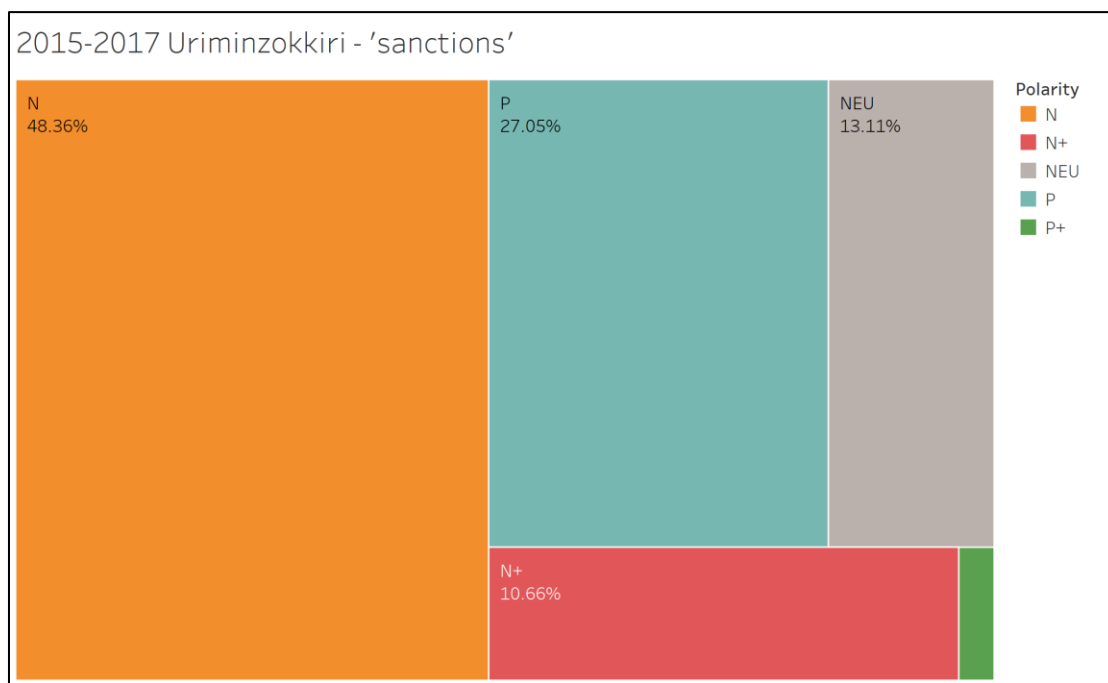


Figure 52: 2015-2017 Uriminzokkiri - 'sanctions'

Diplomacy

Perhaps aided by the longer period of reporting, the diplomacy category for Uriminzokkiri found and includes three related UN resolutions: 2270 (as above), 2321, and 2371. All of the resolutions present the same problem as mentioned above however – they contain elements of diplomacy (condemning the North, urging it to refrain from further nuclear testing, etc.) and economic sanctions (with later resolutions generally strengthening sanctions introduced in previous

resolutions). Even with that combination of tools however, negative sentiment is only 48%, less than the 59% for sanctions alone – a finding the opposite of above, where the Rodong Sinmun reporting was more negative on UN resolution 2270 than it was on sanctions in general.

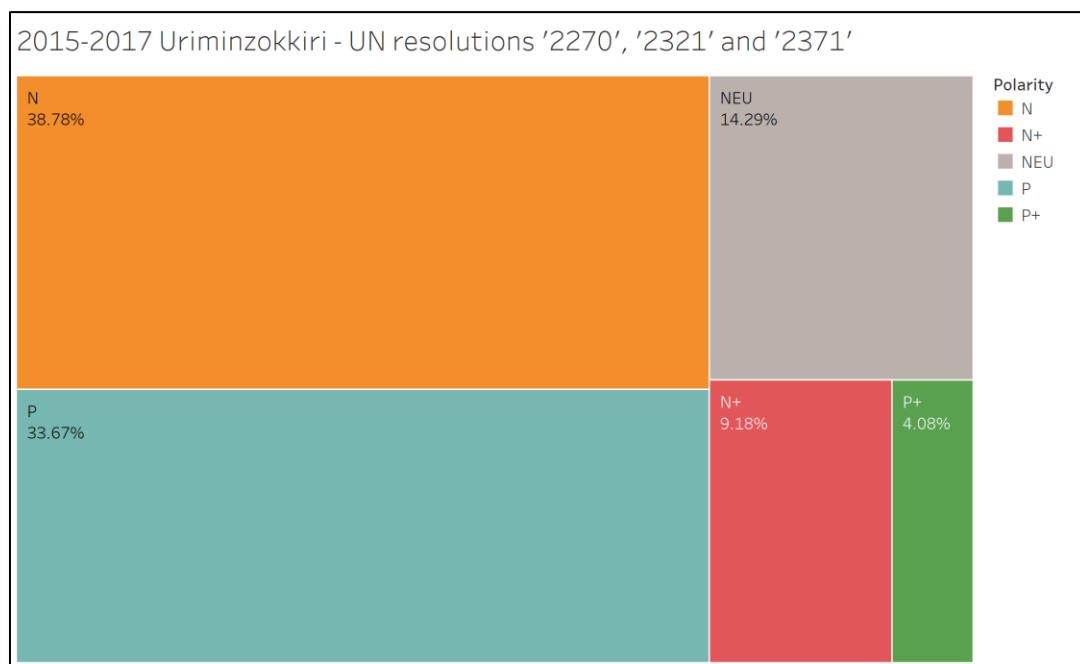


Figure 53: 2015-2017 Uriminzokkiri – UN resolutions '2270', '2321' and '2371'

Information

Finally, in the information category, *loudspeaker* (52%) was again more negative than *psychological warfare* (44%), though with the caveat that the reporting in this category was extremely light, with only one story including *psychological warfare* and three containing *loudspeaker*. The psychological warfare story is from August 2015, the three loudspeaker stories are from August 2015 (two stories) and February 2017.

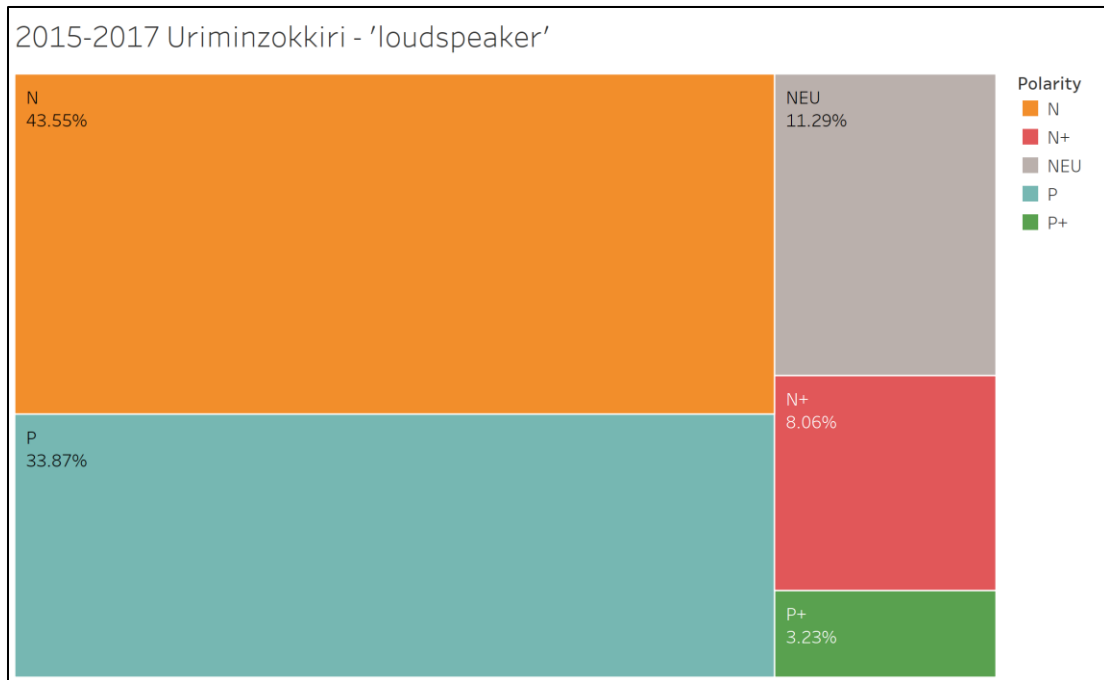


Figure 54: 2015-2017 Uriminzokkiri – 'loudspeaker'

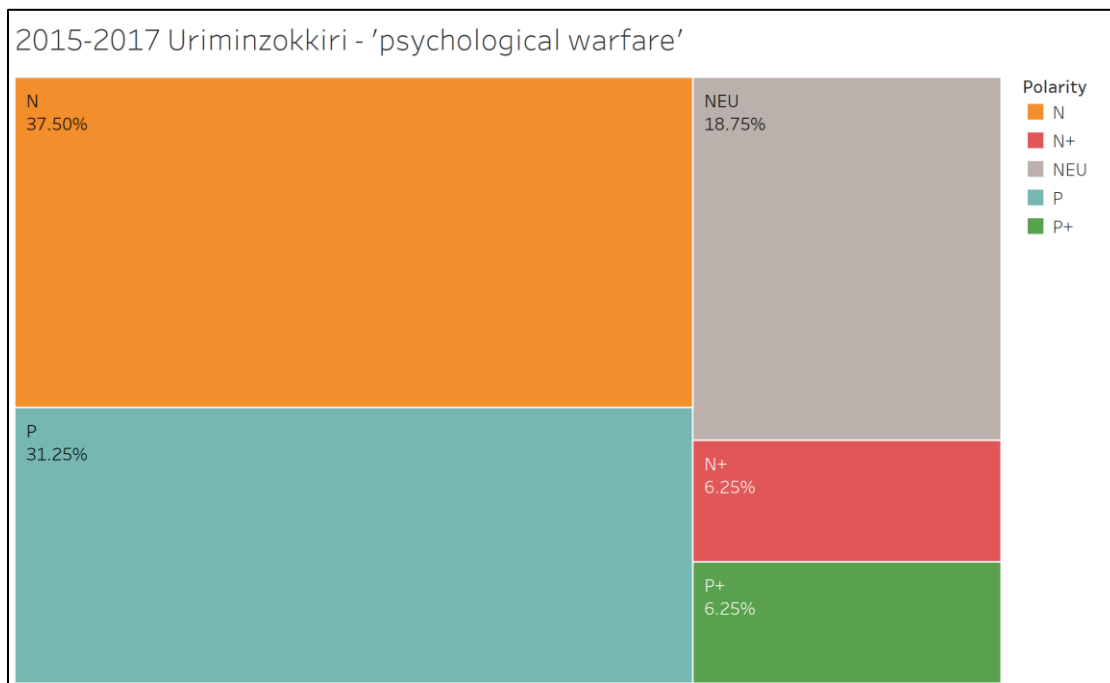


Figure 55: 2015-2017 Uriminzokkiri – 'psychological warfare'

These findings, though limited, place the information category behind the named military exercises and *sanctions*, with *psychological warfare* even behind the diplomacy category, in terms of negative sentiment. Reporting for three of the searches (*ulji*, *loudspeaker*, and *psychological warfare*) was limited. All of the categories were more negative than the baseline, all articles, reporting.

The findings here do not support the hypothesis that authoritarian states react most negatively to pressure in the information environment. Instead, the findings fall more in line with what theory would predict – that states respond more negatively to military tools (as represented by geographically-proximate joint military exercises conducted by adversary states) than other tools of statecraft.

KCNA (Korean Central News Agency)

The Korean Central News Agency, as the name implies, is North Korea's key, authoritative media outlet and has been for decades. When the regime wishes to communicate a key message, whether to an external or internal audience, this is normally the chosen medium. As mentioned previously, this research uses a dataset downloaded in late August 2017 of all KCNA reporting from January 2002 to August 2017, just over 100,000 articles. This data was collected by paying an outside vendor, specialist data collection firm ScrapingHub (<https://scrapinghub.com/>) to access, scrape, and download the articles. Web blocking tools prevented the author from directly gathering this information, as was done for the other sources in the paper, but selecting an outside, specialist firm allowed for collection of a much

larger dataset. As above, we will examine the overall dataset first, before looking at each of the DIME categories, again using the same search terms.

As in the baseline Uriminzokkiri reporting, the baseline KCNA reporting is much more positive, at 68% (the sum of the P and P+ reporting), than negative, at 22% (though not visible in the graph below, very negative, N+, sentiment was a relatively miniscule 0.83%). This finding alone is interesting, for it contradicts the common narrative of the North as a cranky, belligerent state, publicly grating to friends (e.g. China, Russia) and verbally hostile to foes (e.g. South Korea, Japan, the U.S.).

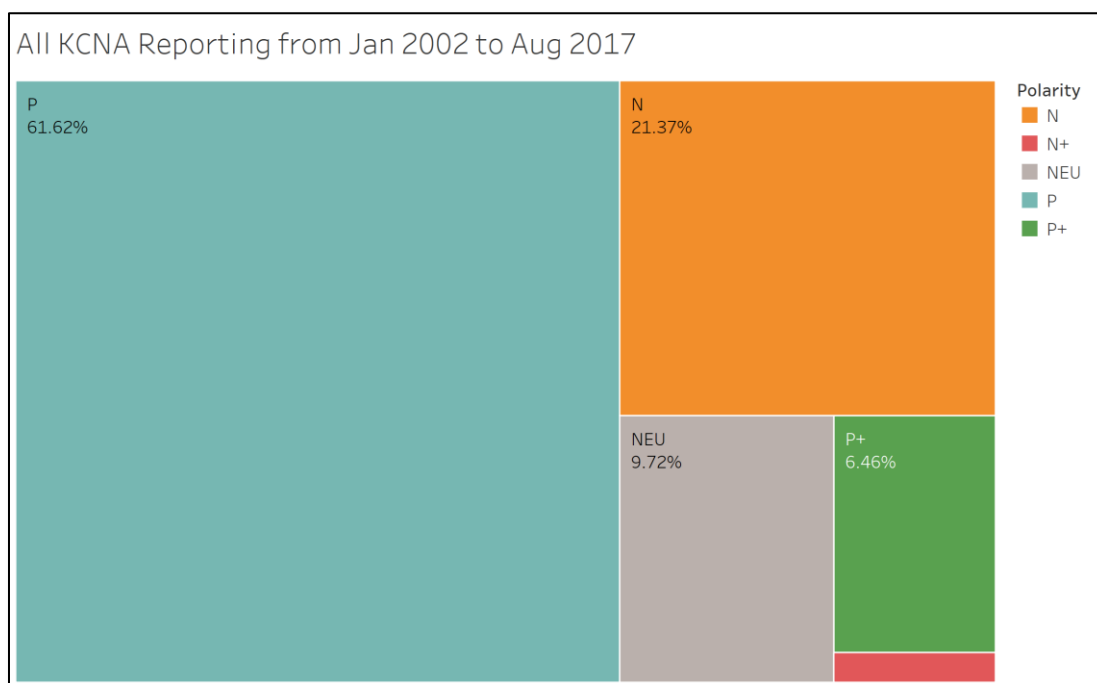


Figure 56: All KCNA Reporting from Jan 2002 to Aug 2017

The same data is shown below, broken down monthly by the polarity and number of reports. Note positive reporting (light blue) is always higher than

negative reporting (orange), and very positive reporting (green) is always higher than very negative (red) reporting. Also note the large spike in overall reporting starting in 2011 and lasting well into 2012.

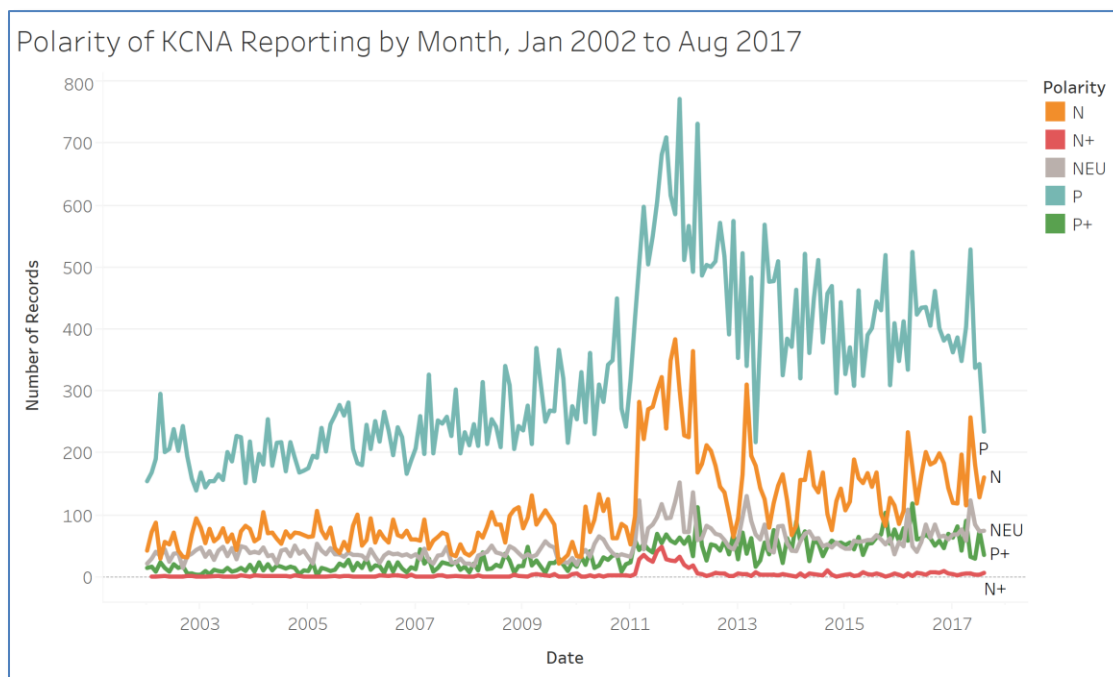


Figure 57: Polarity of KCNA Reporting by Month, Jan 2002 to Aug 2017

The South had National Assembly elections in April 2012 and a presidential election in December 2012, the South Korean naval vessel *Cheonan* was sunk in March 2010 (reportedly by a North Korean torpedo), the shelling of Yeonpyeong Island by the North (with return artillery fire by the South) occurred in November 2010, and Kim Jong-il, North Korea's leader at the time, died in December 2011. While all are important events that occurred on or around the peninsula during this approximate time period, none appear to have correlation or causation with the spike in reporting noted above. The graph below, of month-on-month spikes in

positive or negative reporting, provides additional details of sudden changes in reporting sentiment, but again, none appear correlated with the events noted above.

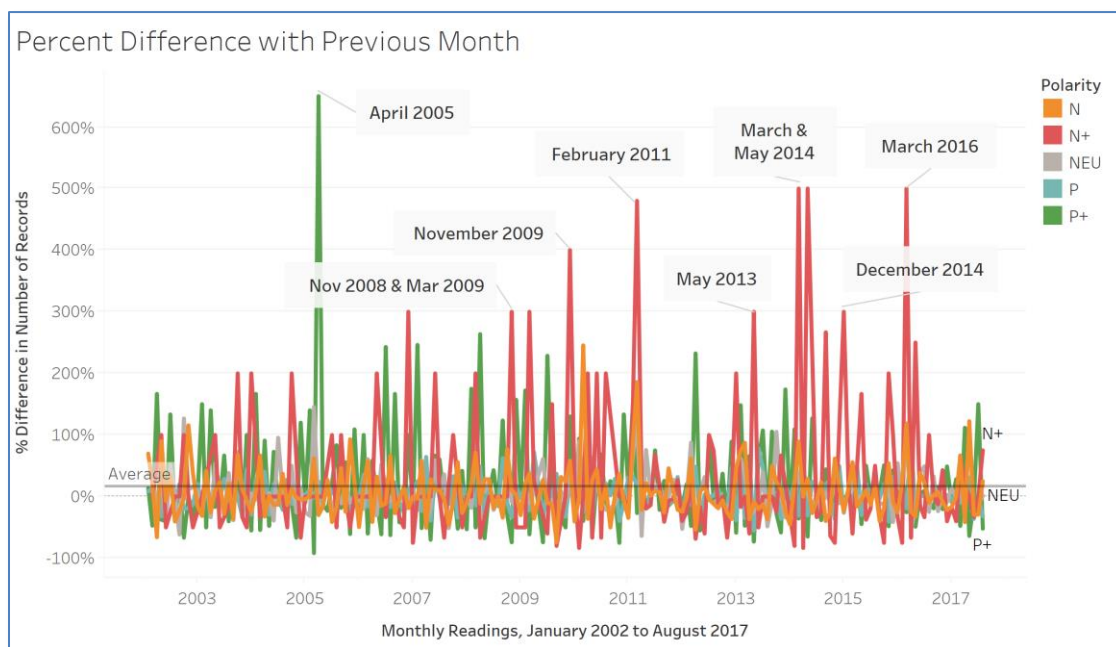


Figure 58: KCNA Reporting, Percent Difference with Previous Month

Next, we turn from this broad overview of KCNA reporting to the DIME category-focused reporting. The two timelines above may prove useful when examining the four categories. This section mainly uses the same terms as above with the Rodong Sinmun and Uriminzokkiri reporting, only with a much larger dataset and, due to the longer timespan, with several additional (i.e. older) UN resolutions.

Military

As in the reporting above, the term *military exercise* was less negative than the sentiment for the two named exercises (Ulji and Foal), though there was less of a

gap in this reporting. The reduced gap could be related to the limited number of stories found for some of the searches above. Below is the KCNA reporting on *military exercise*.

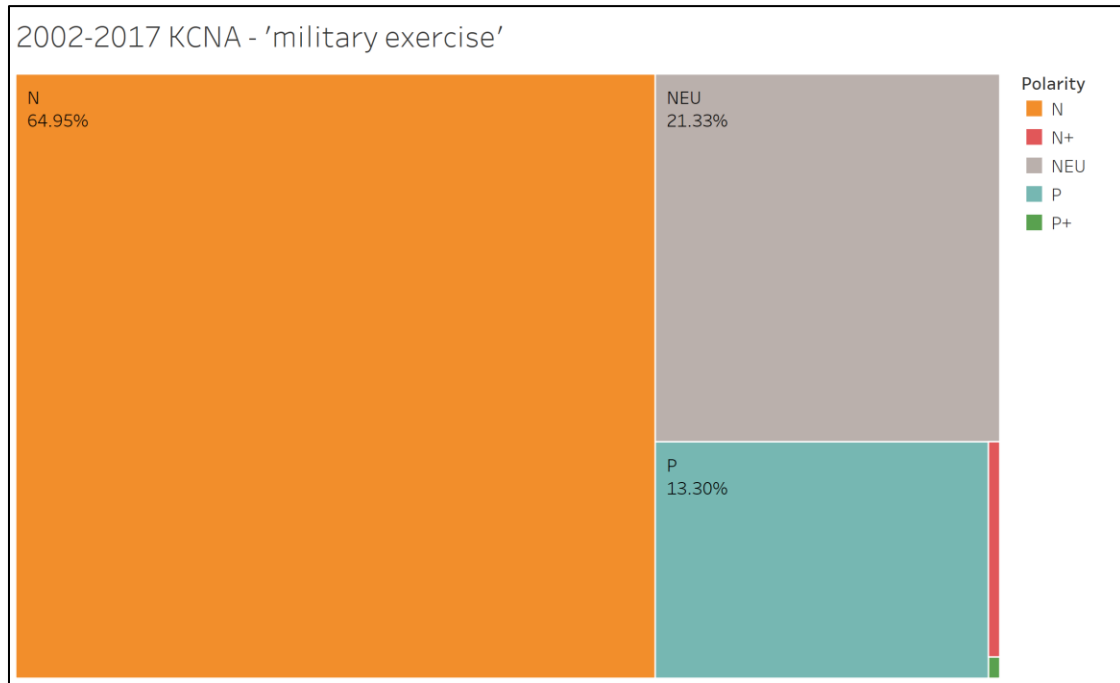


Figure 59: 2002-2017 KCNA - 'military exercise'

Though the amount of very negative (N+) reporting is not visible in the image, at .39% it is negligible. This provides an overall figure for negative reporting of slightly over 65%. For the two named exercises, the negative results are somewhat higher, per below.

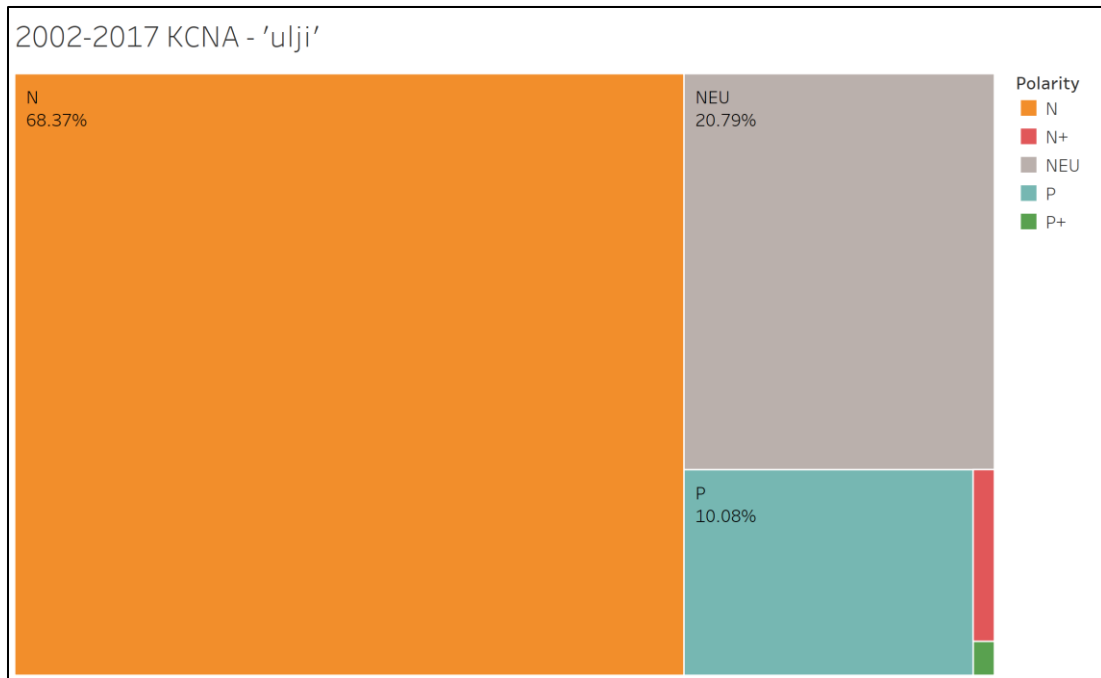


Figure 60: 2002-2017 KCNA - 'ulji'

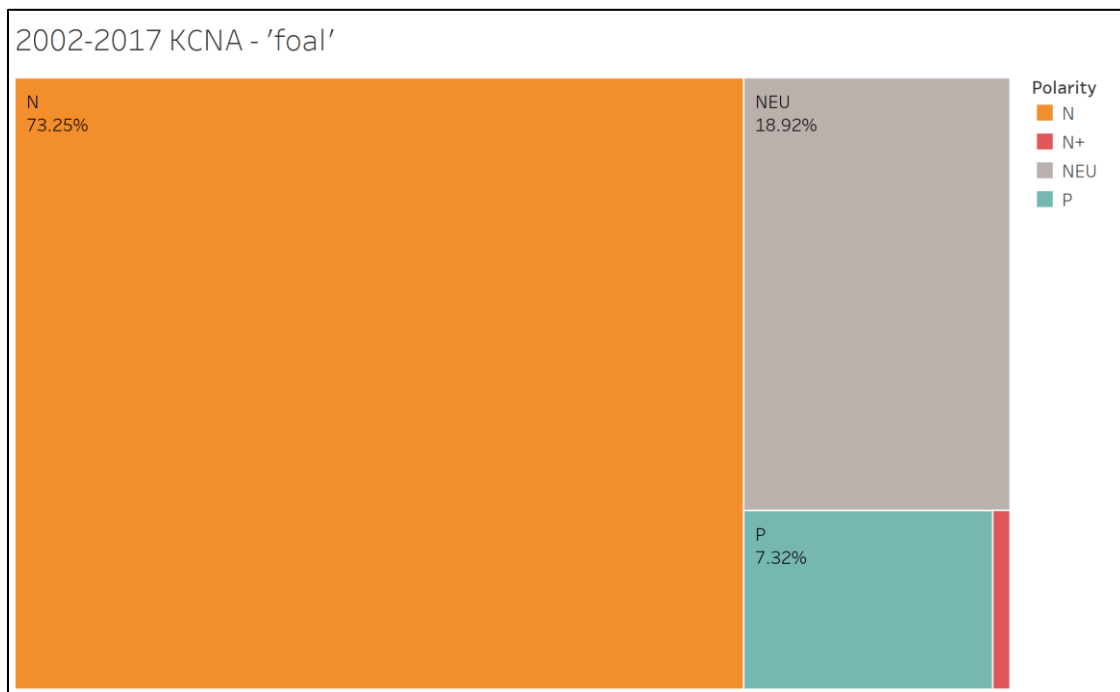


Figure 61: 2002-2017 KCNA - 'foal'

The negative sentiment for Ulji Focus Lens (or Ulji Freedom Guardian) is just under 70%, while that for the Foal Eagle exercises is 74% – both among the highest levels found in this research. These results are in line with theory, that military actions/threats would be viewed most negatively by the targeted state(s).

Additional support for realist approaches comes from the data below, showing negative sentiment by month over the course of a year. If Pyongyang's views on military exercises are indeed quite negative, then all else being equal (as is the case with this dataset), periods with military exercises should have elevated levels of negativity. Fortunately for the research here, joint U.S. – South Korean exercises are nearly always held in March and August, and only in those two months.¹⁸² While a start or end date may occasionally stray outside of those months, the bulk of the annual exercises occur in March and August. With this being the case, March and August should have the most negative reporting compared to months lacking exercises. In the image below, the KCNA data from 2002-2017 is combined, then broken down by polarity (negative, positive, very negative, etc.), by month. The numbers next to the colors each month indicate the ranking of that month's polarity out of all months of the year. So, for example, a number 1 next to orange in March would indicate March has the highest level of negative sentiment out of any month of the year, for all years combined from 2002-2017.

¹⁸² "Beyond Parallel." Beyond Parallel [database], Center for Strategic and International Studies.



Figure 62: 2002-2017 KCNA Monthly Aggregate Sentiment

Though somewhat complex, the graphic above shows March has the most negative sentiment (N) of any month, with August having the third most negative. In terms of very negative (N+), August is first and March is second. Interestingly, positive (P) sentiment is highest in April and September – the two months directly *after* the exercises complete. This finding supports the idea that Pyongyang responds very negatively to the annual joint U.S – South Korean military exercises. This finding, so clearly indicative of the North’s concern with the military exercises, is one of the key findings of the paper.

It is important to point out here that other researchers have found this to *not* be the case, that instead, Pyongyang’s reactions to the annual exercises are based more on the then current relations with the U.S. than actual sentiment toward the specific exercises. “A new study by *Beyond Parallel* shows that annual U.S.-ROK [Republic of Korea] military exercises [...] do not provoke North Korea. The study’s findings demonstrate that these summer/fall exercises, like the spring Foal Eagle and Key Resolve exercises, have a ‘null effect’ on North Korean provocations from 2005 to 2016. This is despite periodic claims by Pyongyang and the media that these annual military exercises provoke North Korean belligerence.”¹⁸³

“According to *Beyond Parallel* original datasets, the state of U.S.-North Korea diplomatic relations before the exercise period (defined as 4-8 weeks prior) is actually a better indicator of whether North Korea will carry out provocations during or after the exercises. In the study, if U.S.-DPRK bilateral relations were coded positively prior to the exercises, the North’s response remains restrained

¹⁸³ Cha, Lee, and Lim, DPRK Provocations and US-ROK Military Exercises, 2005 to 2016”.

both during and after the exercises. If pre-exercise relations were coded negatively, then there is a higher likelihood of North Korean belligerence during and after the exercises.”¹⁸⁴

Rather than sentiment, the study cited above focuses on North Korean actions (termed “provocations” by the study) during and after the exercises, which may account for the different findings. Whether North Korean sentiment related to the exercises also varies based on the positive/negative coding for U.S. – North Korea relations prior to the exercises appears an interesting area for future research.

Economic

As above, the term *sanction* was used as a proxy for North Korea’s response to outside entities targeting it with economic sanctions. Interestingly, there was almost no very negative (.18%) or very positive (.15%) sentiment expressed in the reporting, as shown below.

¹⁸⁴ Cha, Lee, and Lim, DPRK Provocations and US-ROK Military Exercises, 2005 to 2016”.

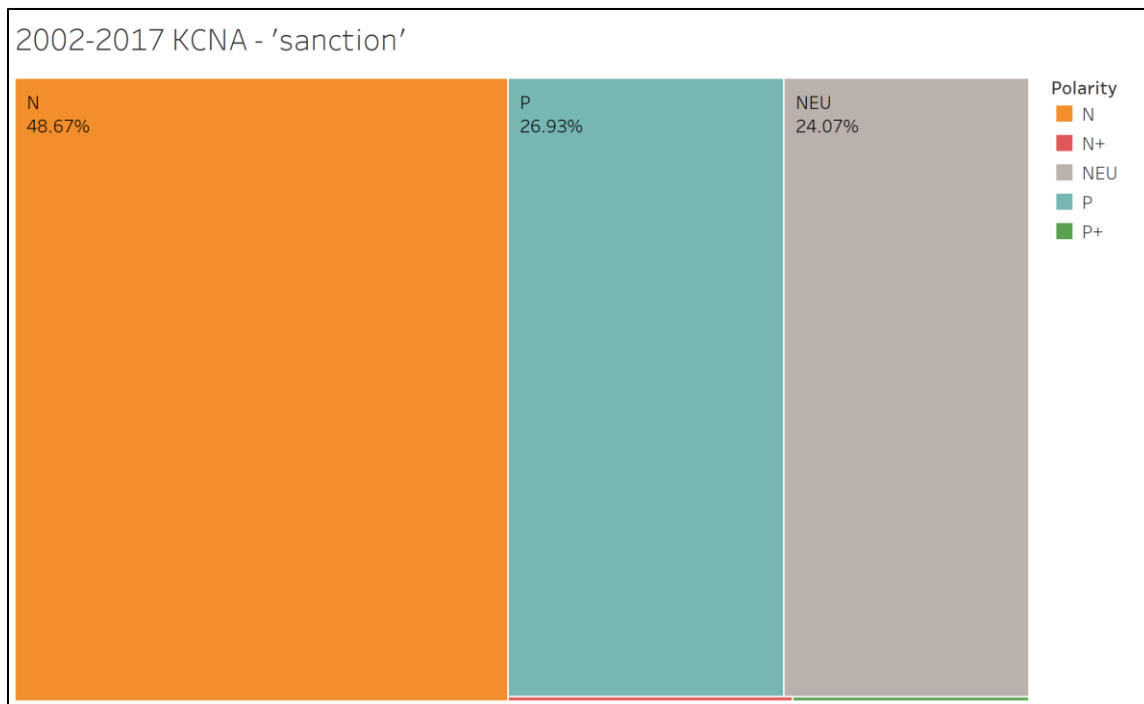


Figure 63: 2002-2017 KCNA – ‘sanction’

At 49%, this finding is in line with previous findings that show the North responds less negatively to economic sanctions than it does to the military and information tools of statecraft. Next, we examine the North’s reaction to a number of different UN resolutions, nearly all of which combined both diplomatic censure and remonstrations with economic sanctions.

Diplomatic

Thanks to the greater length of time available in the KCNA data, the research was able to look at not only UNSC resolutions 2270 (also examined under Rodong Sinmun and Uriminzokkiri) and 2371 (also examined under Uriminzokirri), but also older resolutions 1718 (from 2006), 1874 (2009), and 2087 (2013). First is a graph

showing reaction to all diplomatic efforts (UN resolutions 1718, 1874, 2087, 2270, and 2371) combined, followed by separate graphs looking at each resolution independently.

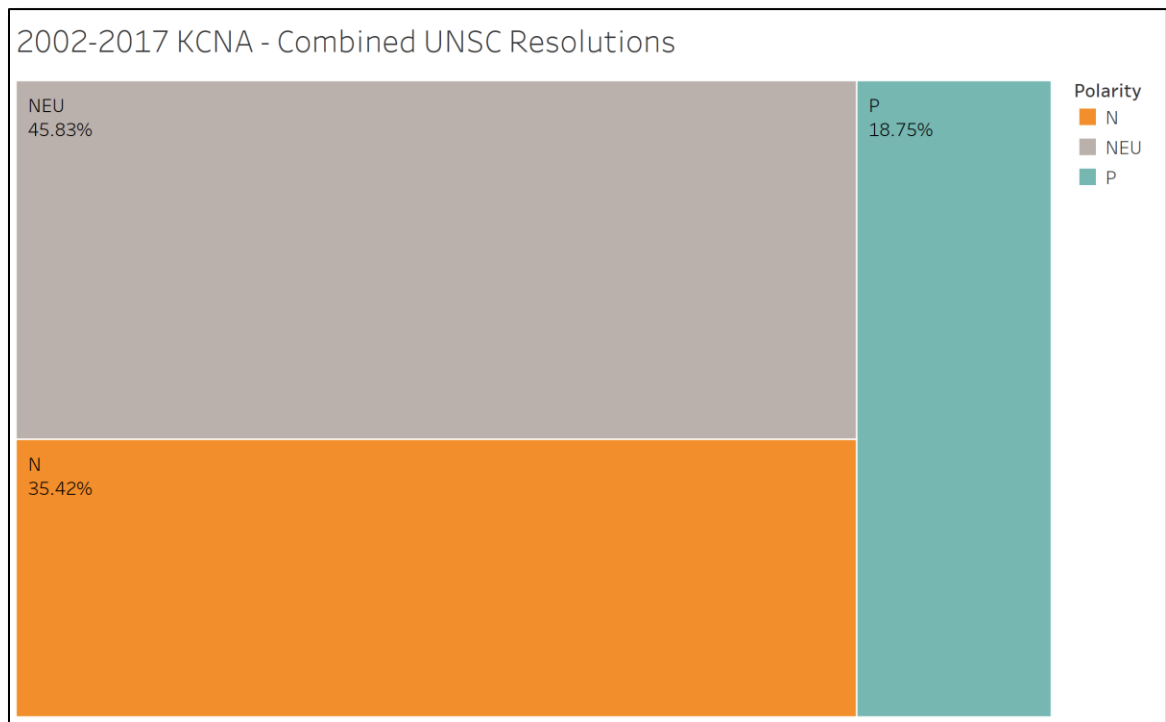


Figure 64: 2002-2017 KCNA – Combined UNSC Resolutions

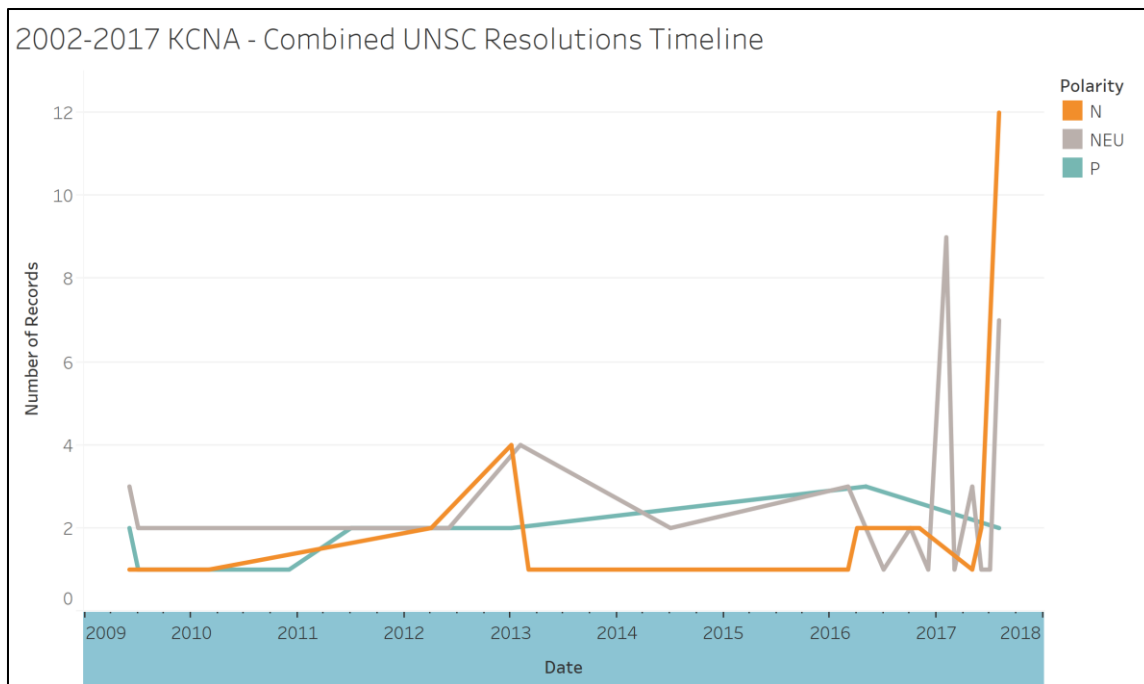


Figure 65: 2002-2017 KCNA – Combined UNSC Resolutions Timeline

Two unique points are evident in the data above. First, there is no *very negative* or *very positive* sentiment for any of the resolutions throughout the entire 15-year time period examined. Second, neutral sentiment often, and overall, outweighed positive or negative sentiment. While some resolutions generated predominantly negative sentiment, as we will see below, the overall neutrality and lack of extremes displayed by the diplomatic-focused data is unique and merits future research attention.

Next, we examine the resolutions individually, from oldest to most recent. The first, UNSC Resolution 1718, was passed on 14 October 2006, expressed “grave

concern” over North Korea’s nuclear program/test, and imposed sanctions.^{185 186}

Noting this, the resolution is a combination of both diplomatic and economic tools.

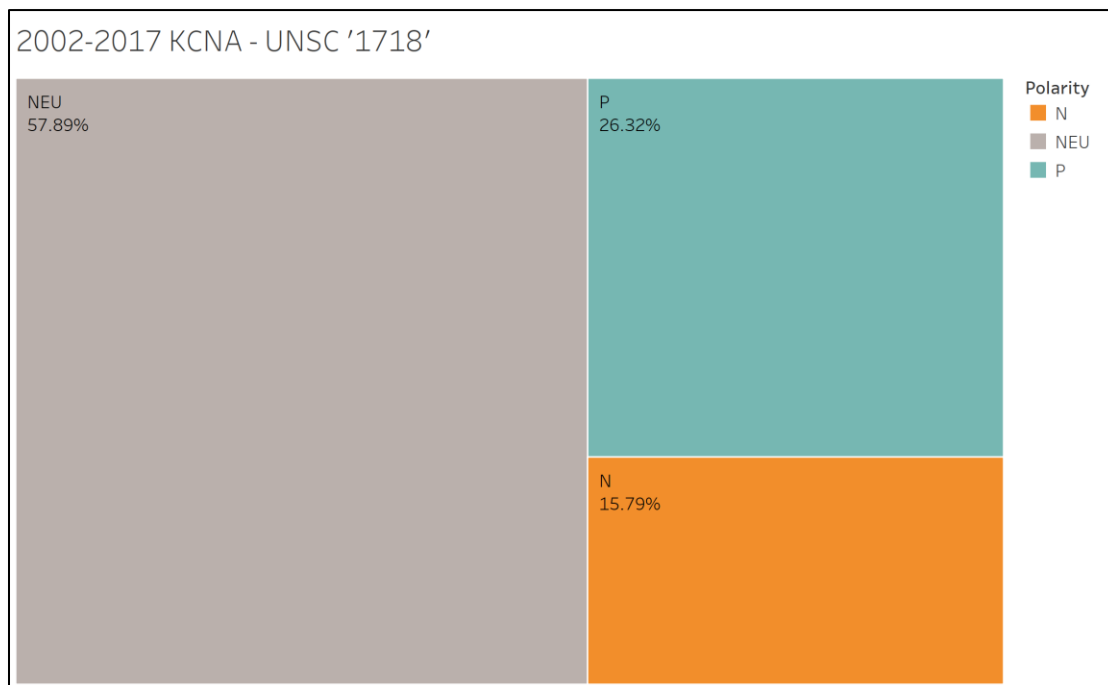


Figure 66: 2002-2017 KCNA – UNSC 1718

The main sentiment expressed in reaction to this resolution is neutral, with negative sentiment the least expressed. As we will see throughout this section, neutral sentiment is often quite large, especially in comparison to the other sections and media outlets examined. Additional research is required to understand why this outcome was so neutral, especially given the combination of two tools of statecraft.

¹⁸⁵ Security Council Report, UN Documents for DPRK (North Korea), accessed 9 January 2018.

¹⁸⁶ UN, Security Council. “SECURITY COUNCIL CONDEMNS NUCLEAR TEST BY DEMOCRATIC PEOPLE’S REPUBLIC OF KOREA.” Resolution 1718 (2006).

The next resolution in our chronological order is UNSC Resolution 1874, from 12 June 2009, which greatly expanded sanctions on the North, while again expressing “grave concern” in response to a nuclear test conducted by the North.¹⁸⁷ ¹⁸⁸ This resolution is also an example of both economic and diplomatic tools being used to pressure the North, with this one arguably containing tougher sanctioning terms.

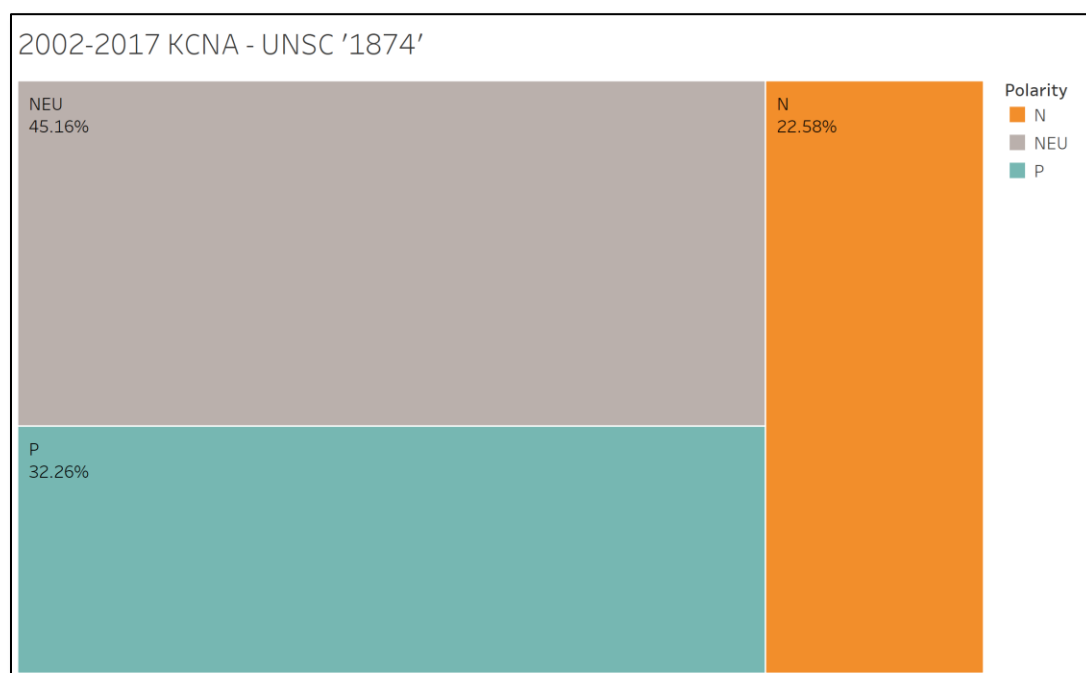


Figure 67: 2002-2017 KCNA – UNSC 1874

Again, the results here show neutral as the most common sentiment expressed, with negative as the least-expressed. The next resolution, 2087, shows Pyongyang reacting more in line with expectations, with negative becoming the

¹⁸⁷ Security Council Report, UN Documents for DPRK (North Korea), accessed 9 January 2018.

¹⁸⁸ UN, Security Council. “Security Council Condemns Democratic People’s Republic of Korea Nuclear Test, Toughens Sanctions.” Resolution. 1874 (2009).

dominant sentiment. This resolution differs from the previous two in at least two aspects, it occurred after Kim Jong-il had died (December 2011) and his son Kim Jong-eun had taken power in the North, and two, it came in response to a ballistic missile launch/test rather than a nuclear test. As with the other resolutions however, 2087 combines both sanctions and diplomatic pressure.^{189 190}

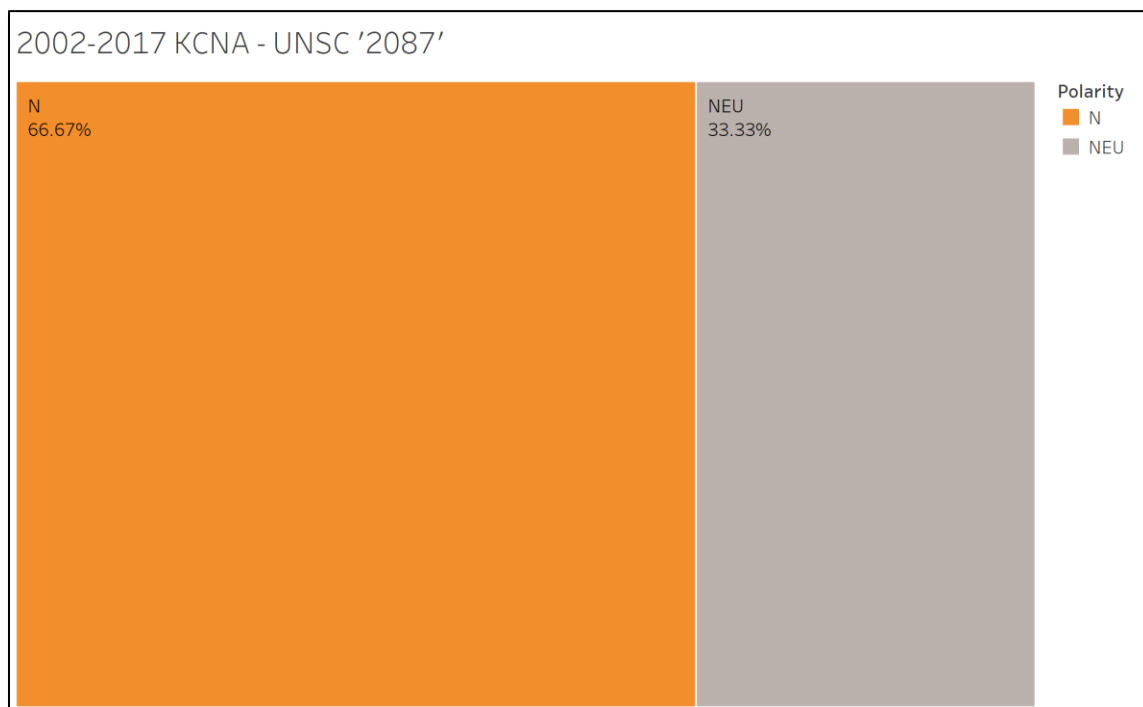


Figure 68: 2002-2017 KCNA – UNSC 2087

North Korea’s response here was much more negative than with previous resolutions, with no positive sentiment at all and negative sentiment at nearly 67% – even more negative than with *military exercise*. This result is an outlier compared to the other reactions to Security Council resolutions.

¹⁸⁹ Security Council Report, UN Documents for DPRK (North Korea), accessed 9 January 2018.

¹⁹⁰ UN, Security Council. “Security Council Condemns Use of Ballistic Missile Technology in Launch by Democratic People’s Republic of Korea, in Resolution 2087 (2013).”

The next resolution, UNSC 2270 from March 2016, again combines diplomatic pressure with economic sanctions, condemning the North for violating previous resolutions by conducting a nuclear test and using ballistic missile technology.¹⁹¹ ¹⁹² However, as we can see below, the North's response is again predominantly neutral. This is different from the Rodong Sinmun and Uriminzokkiri reporting on the same resolution, which was much less neutral, though contained similar levels of negative sentiment.

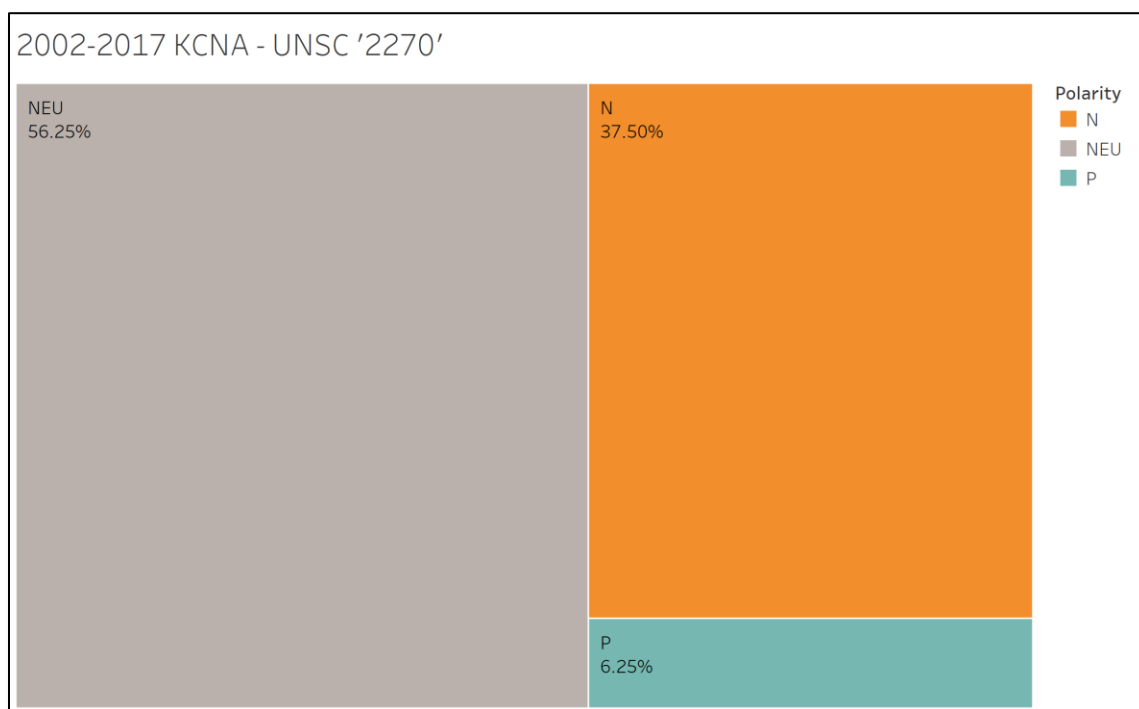


Figure 69: 2002-2017 KCNA – UNSC 2270

Finally, the last resolution is UNSC Resolution 2371, from August 2017. This resolution again toughened sanctions and condemned North Korea's use of ballistic

¹⁹¹ Security Council Report, UN Documents for DPRK (North Korea), accessed 9 January 2018.

¹⁹² UN, Security Council. "Security Council Imposes Fresh Sanctions on Democratic People's Republic of Korea, Unanimously Adopting Resolution 2270 (2016)."

missile technology.^{193 194} Like resolution 2087, above, 2371 focuses on punishing the North for ballistic missiles, rather than nuclear tests. Also, as shown below, 2371 has more negative than neutral sentiment.

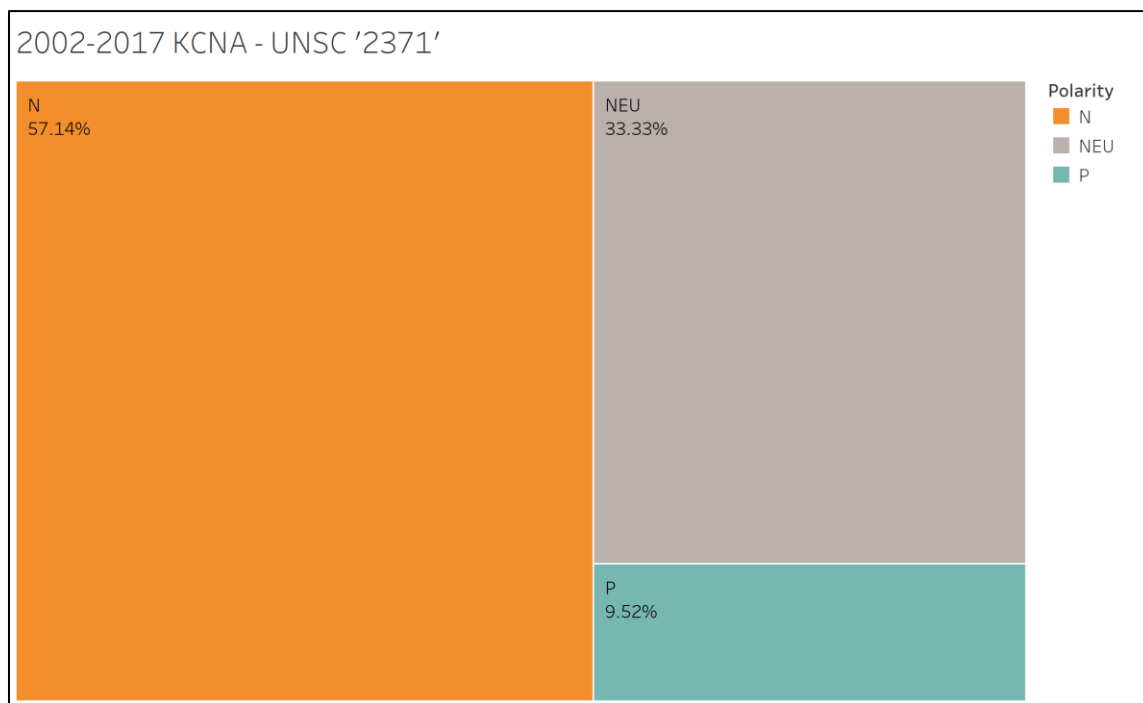


Figure 70: 2002-2017 KCNA – UNSC 2371

While two testcases contain too limited of a dataset to draw conclusions, the only UN resolutions surveyed here that focused on missiles, rather than nuclear tests, were also the only two to see negative sentiment jump substantially and outweigh neutral sentiment. If these examples were to hold true under additional testing, a finding that the North reacts more strongly to criticism of missile testing than nuclear testing would be an interesting, possibly policy-relevant finding.

¹⁹³ Security Council Report, UN Documents for DPRK (North Korea), accessed 9 January 2018.

¹⁹⁴ UN, Security Council. “Security Council Toughens Sanctions Against Democratic People’s Republic of Korea, Unanimously Adopting Resolution 2371 (2017).”

Overall, the North's response to UN resolutions that combined diplomatic and economic pressure was predominantly neutral, making these measures the least effective of the three tools examined thus far. In only two cases, both focused on missile testing/launches, did negative sentiment actually outweigh neutral sentiment. As mentioned above, this finding merits further research attention.

Information

Finally, the KCNA research turns to the information category, again examining the North's reaction to the use of loudspeakers and what it terms *psychological warfare*. Due to the increased amount of data available in this dataset, the research here was also able to include the term *leaflet*. This is in reference to leaflets sent over the border, normally by balloon, from the South into the North. Additionally, and interestingly, the KCNA reports in this category also turned up a reference to *Reporters without Borders*. In April 2016, a KCNA story referenced *South Korea's* standing in *Reporters without Borders'* rankings, and decried the South's poor performance – the same tactic used by the Russian government to draw human rights attention to adversaries and away from its own performance. Given it was only one reference, it is not included in the research below.

Two notes before viewing the graphs: for the *loudspeaker* search term, curation was necessary to remove a large number of false positives from the search results. The KCNA commonly discusses “agitation teams” sent to the countryside or factories to encourage workers to increase output; these teams often use loudspeakers as part of their work, resulting in their appearance in, and subsequent removal from, the search results here. Additionally, in KCNA parlance, “right-wing

Japanese gangsters” commonly harass the offices of Chongryon (roughly, the general association of Koreans resident in Japan who favor Pyongyang over Seoul) using loudspeakers mounted on vans parked in front of their buildings. These results were also removed from the research.

Second, the term *leaflet* also required manual curation of the data to remove stories discussing the use of leaflets in South Korea and Japan. In both countries, demonstrators commonly distribute brochures and one-page handbills (both often referred to by the term *leaflet* in North Korean media) as part of their demonstrations. Stories referencing these activities were removed from the data.

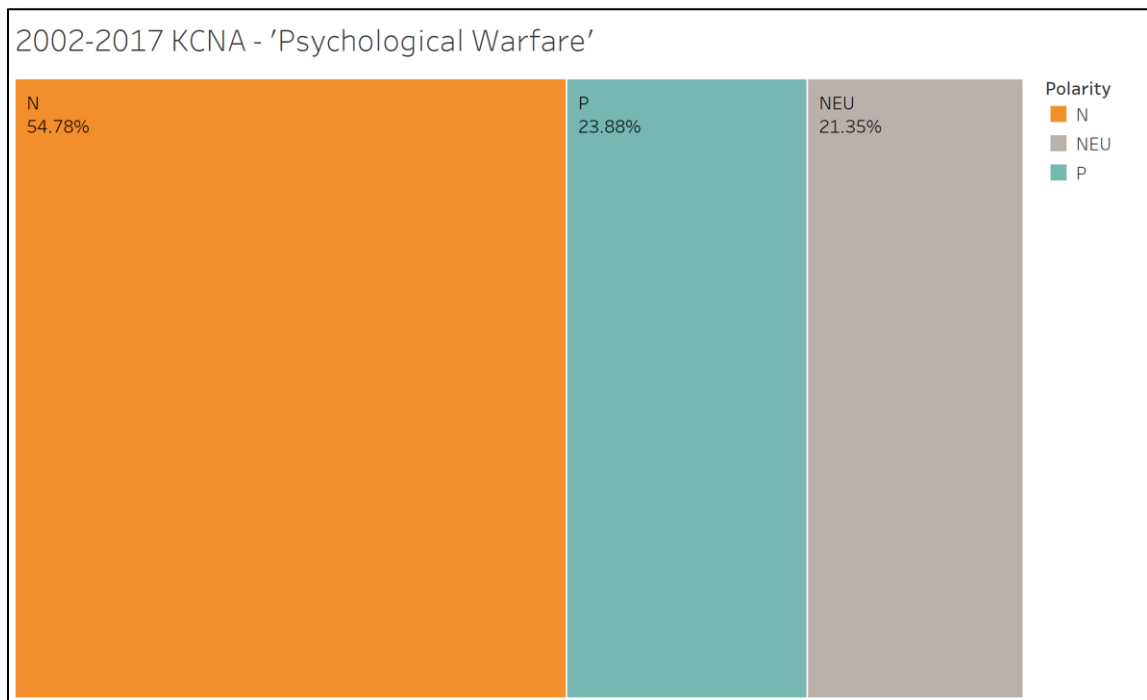


Figure 71: 2002-2017 KCNA - 'Psychological Warfare'

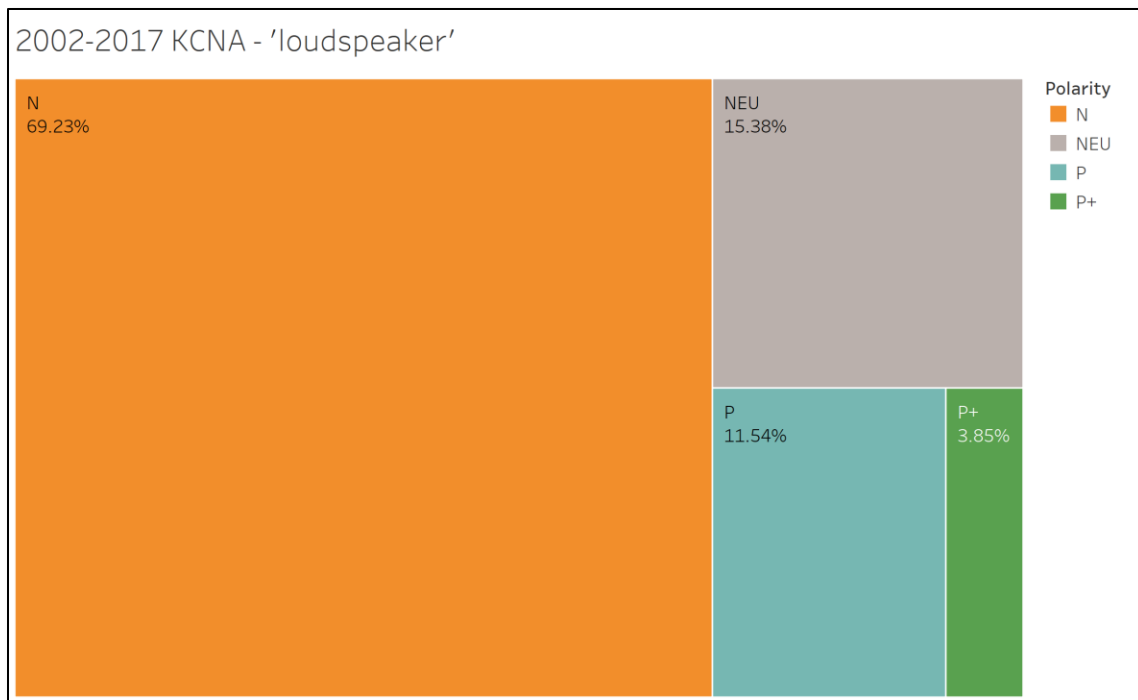


Figure 72: 2002-2017 KCNA - 'loudspeaker'

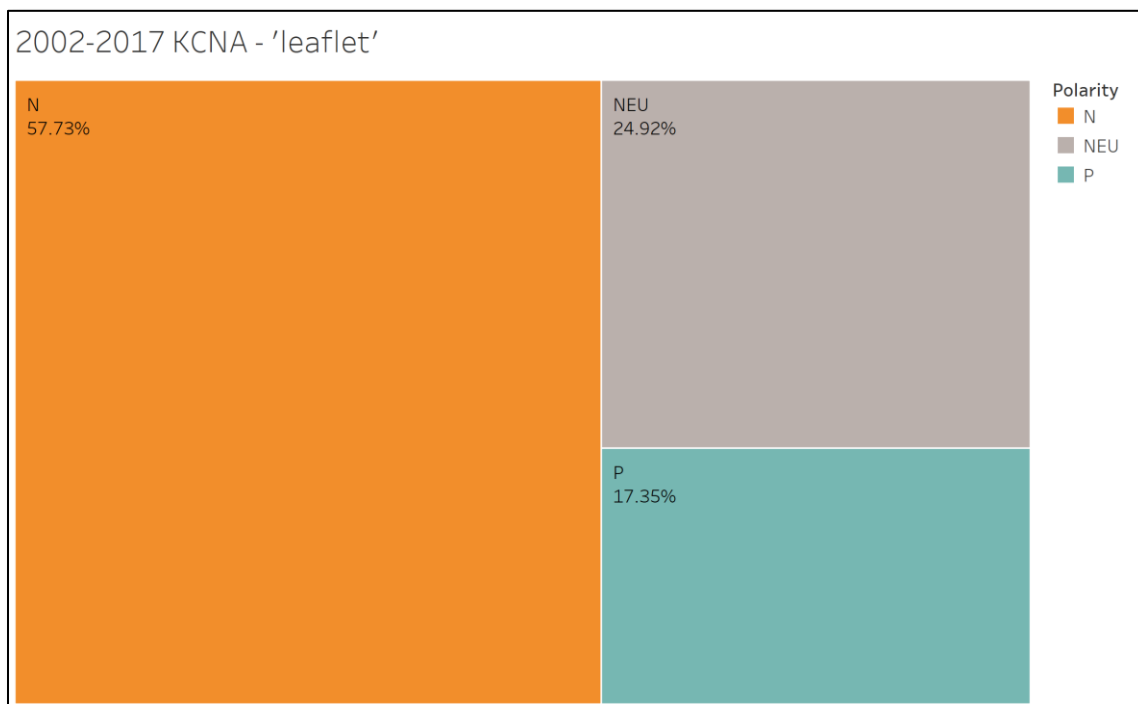


Figure 73: 2002-2017 KCNA - 'leaflet'

From the graphs, *loudspeaker* was again more negative than *psychological warfare*, with *leaflet* in the middle at 58%. While *loudspeaker* remained relatively steady throughout the period surveyed, psychological warfare was much spikier in when it appeared, per the graph below, which also shows a significant negative spike in August 2015 – the month Seoul resumed loudspeaker broadcasts into the North in an (ultimately successful) effort to win some form of apology from Pyongyang for planting landmines that maimed Southern soldiers along the DMZ.

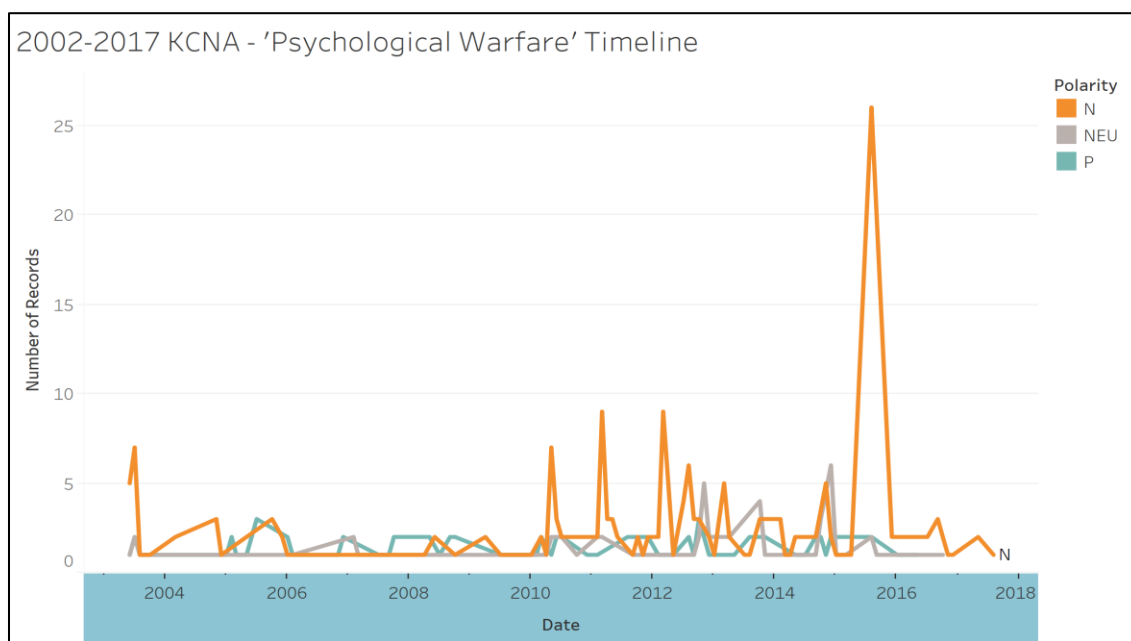


Figure 74: 2002-2017 KCNA - 'Psychological Warfare' Timeline

The timeline for *leaflet* is also interesting, capturing the improvement in relations between North and South in the early 2000s, before turning negative at the end of the decade. The largest spike here is from November 2014, after a 'leaflet-scattering operation' targeting the North was launched in the South, an event which resulted in an exchange of gunfire across the border in October 2014.

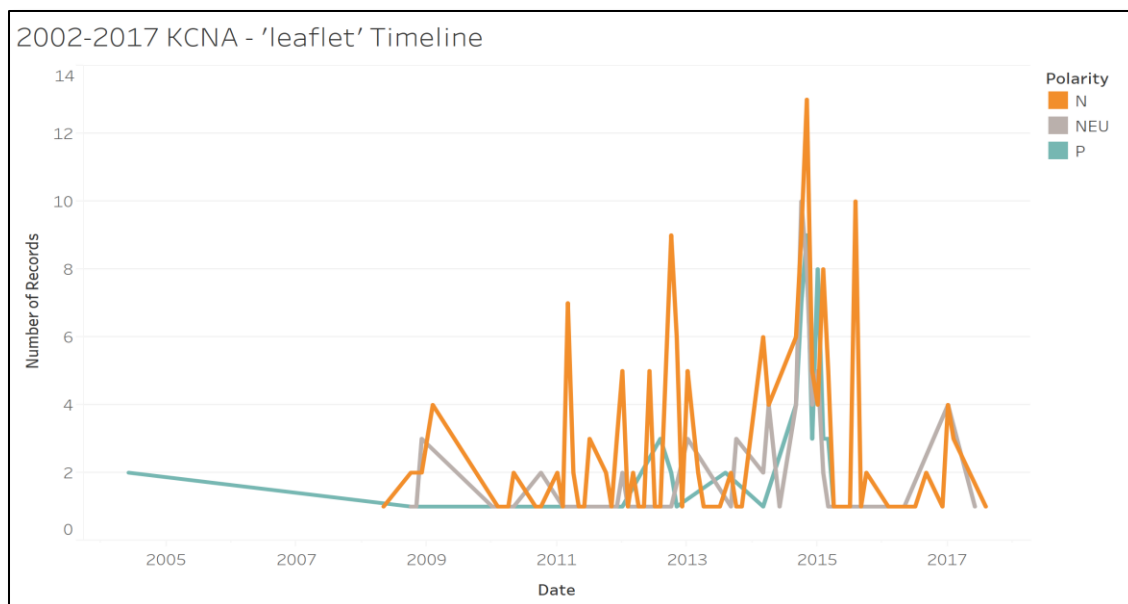


Figure 75: 2002-2017 KCNA - 'leaflet' Timeline

Conclusion

The results here for the KCNA show the named military exercises generated the most negative reaction from the North, specifically the Foal Eagle exercises. The second-highest negative reaction was generated by *loudspeaker*, which garnered a much more negative reaction than sanctions, military exercises, and all of the combined diplomatic and economic search terms (with the exception of resolution 2087, which saw a jump in negativity to 67%, only marginally below *loudspeaker*'s 69%).

While the sentiment, at 58% negative, was not as high for *leaflet* as some of the other terms, it generated a military response from the North that resulted in an exchange of gunfire across the border.¹⁹⁵ Similarly, South Korea's decision to use

¹⁹⁵ Choe, *Koreas Exchange Fire After Activists Launch Balloons Over Border*, 2014.

loudspeakers in August 2015 generated a military response from the North (artillery fire into the South) and led to an exchange of artillery fire across the border.¹⁹⁶ We will look at North Korean actions in response to the four DIME tools in greater detail below, but note here that information tools generated two separate military responses from the North.

The finding that North Korean sentiment is most negative during March and August, the months that normally feature joint U.S. – South Korean military exercises, is one of the key findings of the paper. That sentiment jumps to the most positive levels of the year in the months immediately following the exercises is also an important finding and supports the idea that Pyongyang responds quite negatively to the exercises.

Overall, of the three North Korean state media outlets researched, the findings from Rodong Sinmun and the KCNA support the hypothesis that authoritarian states exhibit a strongly negative reaction to having their information control challenged. The findings from Uriminzokkiri, while also showing reaction to information tools was among the most negative of the terms examined, fell more in line with what theory would predict, that military pressure would generate the strongest negative reaction.

Twitter Data

All three of the official North Korean media outlets examined here maintain a Twitter account: Rodong Sinmun (@rodongsinmun,

¹⁹⁶ Yonhap, (5th LD) *Two Koreas Exchange Shells over Western Border*, 2015.

<https://twitter.com/rodongsinmun>), Uriminzokkiri (@uriminzok, <https://twitter.com/uriminzok>), and the KCNA (@KCNA_KoreanNews, https://twitter.com/kcna_koreannews). However, despite their existence and ease of access (compared to gaining access to some of their related websites), none of the accounts proved useful for this research.

The most recent Rodong Sinmum tweet is from 2011 and the entire account contains a total of only 19 tweets, from 26 December 2011 to the following day, 27 December 2011. Though the most recent KCNA tweet is much newer, from August 2016, there are only a handful of tweets from 2016 before the account jumps back to May 2010 and nearly all of those tweets are simply links back to the main website, with little to no new content. Given the research above already downloaded and examined all KCNA reporting during this time period, little of research value was found on the KCNA Twitter feed.

At first look, Uriminzokkiri appears more promising, with tweets up to the current date (14 January 2018) and prolific for as far back as examined. However, like with the KCNA account, nearly all of the tweets are simply a few words followed by a link back to a story on the main website – there is little to no new content compared to what was downloaded and examined from the website for the research above.

In what may therefore be the least surprising finding of the entire paper, North Korea does not create much content for social media. This greatly reduces the importance of using the social media accounts of the three North Korean media sites examined here, especially once the main websites have been scraped for related

data. Though this may change in the future, for the purposes of this research, North Korean tweets add little value and will not be examined further.

Actions

Enough with the sentiment, what does North Korea actually *do* in response to outside use of the four DIME tools? What data exist on North Korean activities and can any of these activities be linked to outside use of DIME tools? For this section, the research focus will be ‘kinetic incidents’ along the border between North and South Korea. We define *kinetic incident* as the use of small arms, artillery, or naval weaponry by at least one side, during the broadest period under survey here, January 2002 to August 2017.¹⁹⁷

According to a database of North Korean ‘provocations’¹⁹⁸ maintained by the *Beyond Parallel* research project at the Center for Strategic and International Studies, kinetic incidents as they are defined here took place 22 times between 2002 and August 2017.¹⁹⁹ The most recent incident occurred in August 2015, meaning approximately two incidents occurred per year from 2002-2015 (a November 2017 incident of shots fired by the North at one of its soldiers attempting to escape across the border to the South is outside our timeline).

¹⁹⁷ The KCNA data covers 1 January 2002 to August 2017.

¹⁹⁸ It is important to note that *Beyond Parallel* and CSIS use the term *provocation* for a broad range of North Korean activities (e.g. rocket testing, firing short-range missiles, artillery fire near the DMZ/border) that may simply be part of North Korea’s routine military development, training, and exercise activities and are unrelated to ‘provoking’ outside countries. The research here uses the terms *activity* and *event* to describe similar North Korean activities in order to avoid the deterministic *provocation*.

¹⁹⁹ “Beyond Parallel.” *Beyond Parallel*. Washington, DC: Center for Strategic and International Studies.

From the timeline, we can see 2003 and 2010 each contained six incidents, 2014 contained five, and all other years contained between zero and two. Further below, we can see the incidents broken down by type (color), number, and year.

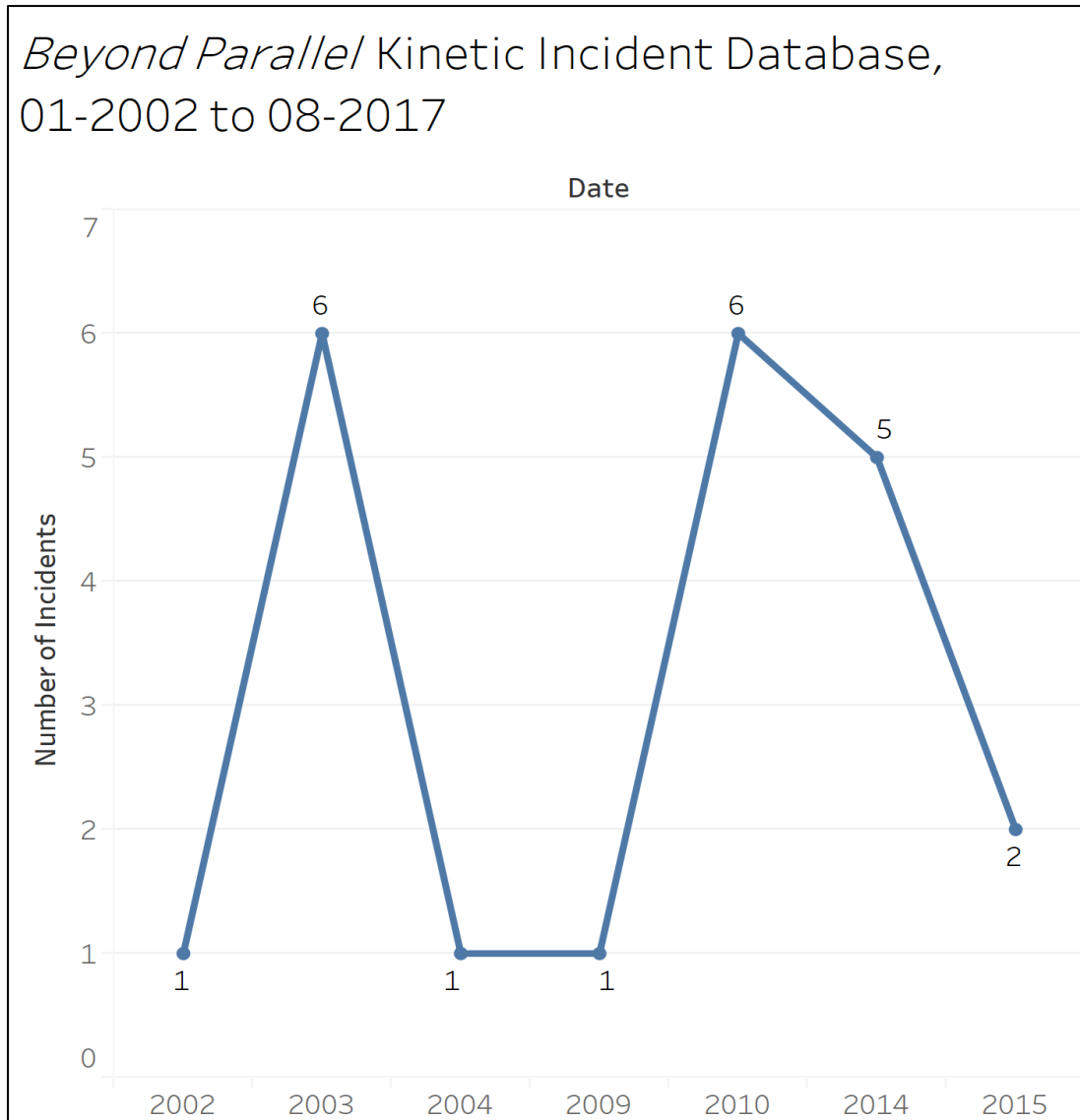


Figure 76: *Beyond Parallel* Kinetic Incident Database, 01-2002 to 08-2017

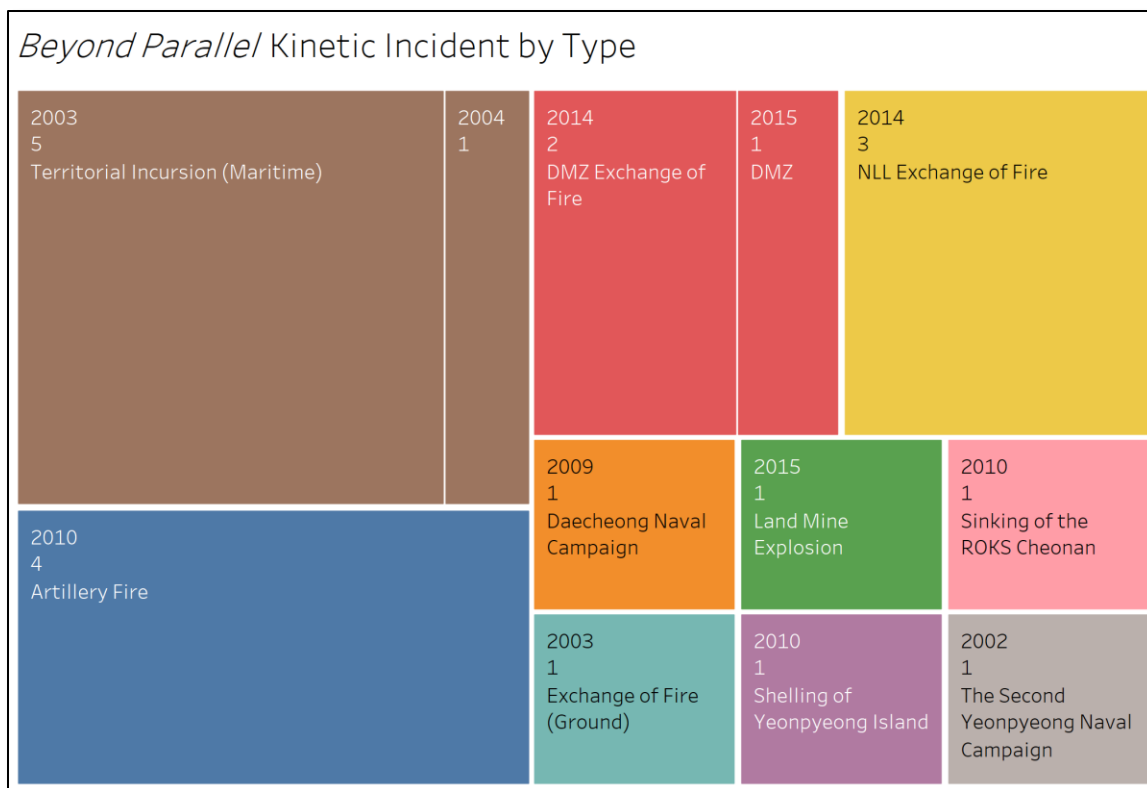


Figure 77: *Beyond Parallel* Kinetic Incident by Type

From the graph, we can see six of the 22 incidents are classified as maritime territorial incursions. This reflects an ongoing dispute between the North and South over the sea border between the two countries in the West (Yellow) Sea. The North does not agree with the current position of this sea border, called the Northern Limit Line (NLL), and both fishing vessels and naval craft from the North routinely travel south of the line and into South Korean waters, most often during peak fishing seasons. These situations are commonly resolved by a show of force, or presence patrol, by South Korean naval vessels. From the data here though, six times the presence of the South Korean vessels (including warnings by ship-mounted loudspeakers) is not sufficient and warning shots were fired (bringing the incident

into the database). For all six incidents here, the warning shots resolved the situation and no further action occurred. Though shots were fired, these incidents are relatively common (North Korean fishing vessels and some naval vessels often are not equipped with state-of-the-art navigation systems and may stray across the border unknowingly) and they resulted in no casualties or property damage. Examination of the incidents finds no reason given or assessed for the incidents' timing or cause, rather, they appear to be part of an ongoing border dispute and unrelated to the use of any DIME foreign policy tools.

Related to the maritime incursions, though more serious, are the three exchanges of fire in the NLL, all in 2014. In these incidents both sides fired at or near the other, though there were no casualties or property damage. Those these incidents were more serious, and could have escalated, there is no reason given or assessed for their timing or cause, rather, they appear to be part of an ongoing border dispute and unrelated to the use of any DIME foreign policy tools.

So far, we have examined nine of the 22 incidents and found no connection to the use of foreign policy tools. The next set of incidents, four episodes of artillery fire (all from 2010), is similar. Each incident appears to involve North Korea conducting artillery drills by firing near and/or into the sea around the NLL. Three of the four incidents occurred in January (on consecutive days from January 27-29), on the heels of November 2009's Daechong Naval Campaign (above, in orange) that saw a North Korean naval vessel damaged (with reports of one North Korean sailor killed and three wounded) after crossing the NLL into the South's waters and engaging

South Korean naval vessels.²⁰⁰ Based on this timing, and lack of a reoccurrence, these four (a similar exercise/incident occurred in August 2010) artillery incidents can be assessed as a warning for the South and training for the North's forces in case they are needed to support a future engagement. Making these four incidents, like the nine already examined, more related to a disputed border than the use of a particular foreign policy tool. The Daecheong Naval Campaign, which resulted in North Korean casualties and likely produced the follow-on artillery incidents, was also due to the disputed border. The timing of the incident, a week before President Obama was due to start a week-long visit to Asia, including meetings with the South Korean president to discuss North Korea's nuclear weapons program, may therefore have a connection to diplomacy, but the tie is unclear.²⁰¹

So far, of the 14 incidents examined, there is one possible, though tenuous connection to diplomacy. The next category of incidents, exchanges of gunfire in the DMZ, changes that, finally bringing a clear connection to one of the DIME categories. The 20 August 2015 exchange of artillery fire in/around the DMZ, the most recent incident in our dataset, was an explicit North Korean response to, and targeting of, loudspeakers the South had started using to broadcast across the border.²⁰² The South's use of the loudspeakers, which had been silent for years under a previous North-South agreement during sunnier times on the peninsula,²⁰³ came as a response (and in order to influence the North to apologize for), the early August

²⁰⁰ Choe, *Korean Navies Skirmish in Disputed Waters*, 2009

²⁰¹ Choe, *Korean Navies Skirmish in Disputed Waters*, 2009

²⁰² Choe, *North and South Korea Trade Fire Across Border, Seoul Says*, August 20, 2015

²⁰³ CNN, *Koreas Agree to Military Hotline*, 2004

emplacement of land mines by the North that wounded two South Korean soldiers on the South's side of the DMZ.²⁰⁴ The reason the North placed the mines is unclear, and unlikely due to the outside use of any foreign policy tools.

In addition to the attack over the loudspeakers, the exchanges of fire in the DMZ also included a 10 October 2014 exchange when North Korean soldiers fired small arms (machine guns) at leaflet-filled balloons being sent into the North from the South by an NGO. South Korea responded by engaging with its own machine guns.²⁰⁵ Prior to the engagement, the North had warned the South, saying Pyongyang would consider their launch "a declaration of war."²⁰⁶ As with the loudspeaker incident discussed above, this incident is a response to the use of information as a tool to influence the North.

The final exchange of fire in the database occurred nine days after the incident over the leaflets. In this case, after issuing warnings, the South fired on a group of North Korean soldiers moving toward the South's side of the DMZ on 19 October 2014. The North briefly returned fire, but there were no reported casualties or damage to property.²⁰⁷ Coming so soon after the leaflet balloons and related exchange of fire, this incident may also be linked to the leaflets, though any connection is not explicit.

To this point, out of 18 incidents examined, one had a possible tie to diplomacy, one a possible tie to information, and two had explicit ties to

²⁰⁴ Choe, *South Korea Accuses the North After Land Mines Maim Two Soldiers in DMZ*, August 10, 2015

²⁰⁵ Choe, *Koreas Exchange Fire After Activists Launch Balloons Over Border*, October 10, 2014

²⁰⁶ Choe, *Koreas Exchange Fire After Activists Launch Balloons Over Border*, October 10, 2014

²⁰⁷ Choe, *Gunfire Exchanged across Korean Boundary*, October 19, 2014

information. Next, the research turns to the four remaining incidents: the 2002 Second Yeonpyeong Naval Campaign (in grey in the chart), a 2003 exchange of groundfire (light blue), and 2010's Shelling of Yeonpyeong Island (purple) and Sinking of the ROKS Cheonan (pink). For ease of reference, the chart is shown once more, below.

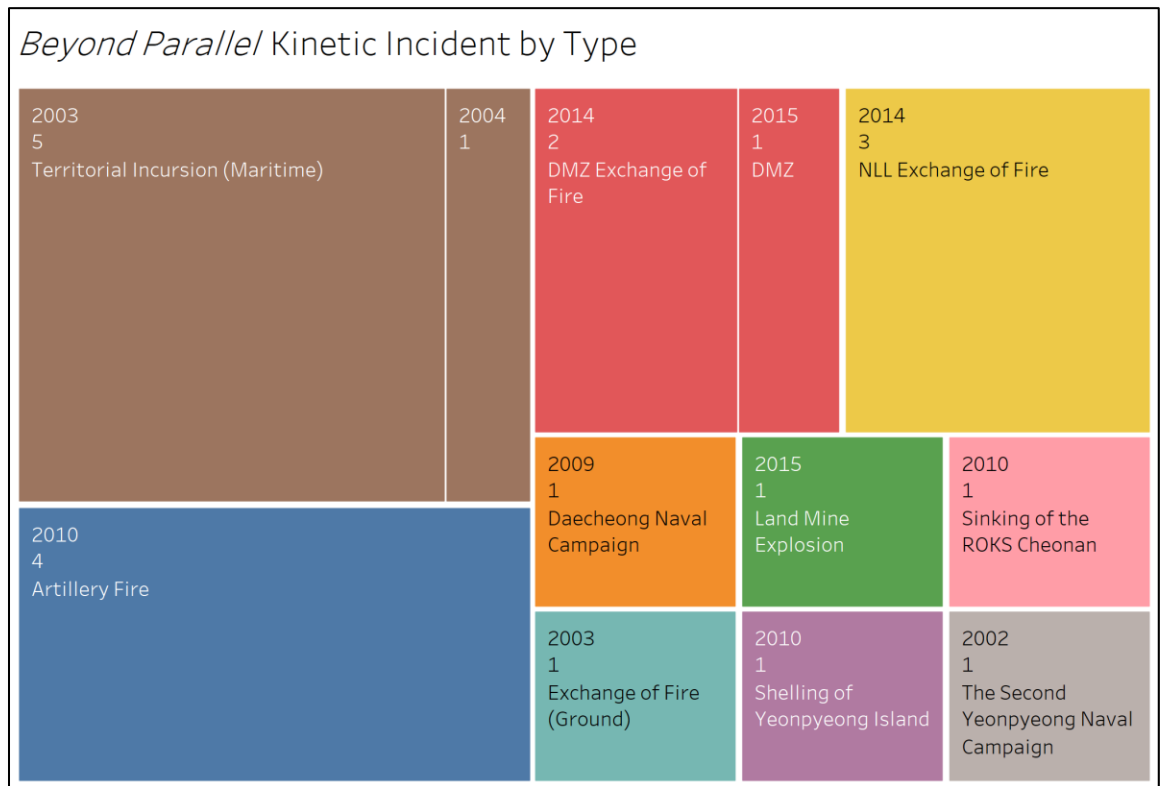


Figure 78: *Beyond Parallel* Kinetic Incident by Type

The Second Yeonpyeong Naval Campaign, 29 June 2002 (the first was in June 1999), was one of the deadliest confrontations between the North and South since the end of the Korean War, with 13 North Koreans reportedly killed and 25

wounded, while the South suffered 6 killed and the loss of a patrol boat.²⁰⁸ This incident also occurred in/around the disputed NLL sea border, but came at a time (2002) of generally better relations between the two countries – though during a peak in the fishing/crabbing season when tensions in the area (as we have seen from the numerous other incidents in this region) run higher than normal. It is unclear what caused this incident, but it does not appear related to the use of a foreign policy tool.

Next, a 17 July 2003 exchange of groundfire in/near the DMZ that resulted in no casualties for either side, is also unclear as to cause. KCNA records show no statement on the incident by the North, with the timing apparently unrelated to any outside activities.

Finally, 2010 saw two deadly incidents between the North and South. First was the March sinking of the South Korean naval corvette Cheonan by a torpedo, assessed to have been fired by the North. The ship was just south of the NLL at the time it was attacked, but the North denied involvement. No clear assessment has emerged for why the attack occurred. 2010's second incident, the Shelling of Yeonpyeong Island, once again involved an area near the disputed NLL sea border. In this incident, North Korea shelled an island in the South, Yeonpyeong, near the NLL, killing four South Koreans and wounding others, while an unknown number of North Koreans were wounded or killed after South Korean Marines returned artillery fire.²⁰⁹ This incident, occurring a few months after the sinking of the

²⁰⁸ "Beyond Parallel." Beyond Parallel. Washington, DC: Center for Strategic and International Studies.

²⁰⁹ Yoo, *Marines Recall Yeonpyeong Shelling with Anger, New Perspective*, November 21, 2011

Cheonan and several maritime incursions by the North across the NLL, is also unclear as to cause. As one of the few times the North has targeted a civilian area of the South since the end of the Korean War, it is a serious incident but lacks a clear motive.

From this examination of kinetic incidents between the North and South from 2002-2017, several points are clear:

1. Nearly all of the incidents occurred in and around the disputed sea border between the North and South
2. 2010 was clearly the peak year in terms of both the number of incidents and their seriousness, with the sinking of the Cheonan and the artillery barrage of Yeongpyeong Island killing 50 and wounding at least 16 in South Korea alone²¹⁰
3. Most importantly for the research here, only 2 of the 22 incidents can be explicitly tied to a foreign policy tool; in this case, the information category, as the North reacted violently to South Korean leaflets and loudspeakers. Two other incidents have possible ties to a category, one to diplomacy and one to information, but lack the explicitness of the loudspeaker and leaflet incidents.

Conclusion

²¹⁰ The sinking of the Cheonan killed 46 South Korean sailors (see: Fifield, *S. Korea Agrees to End Broadcasts as North Expresses Regret for Provocations*, August 24, 2015); the shelling of Yeonpyeong was responsible for the remaining casualties.

The findings in the North Korea section, like in the section on Russia, clearly support the idea that information can be used as a tool of foreign policy at least on par with more traditional tools when it comes to states that seek to control their domestic information environment. In the sentiment analysis of North Korean state media, information tools were second only to specific military exercises in their impact (and first by one measure, the Rodong Sinmun reporting). In the actions category, only the information tools, both loudspeakers and leaflets, were directly tied to inducing a violent North Korean reaction.

These findings, from both the sentiment analysis of North Korean state media and the analysis of violent North Korean actions, provide new contributions to the study of North Korea. In addition, the findings align with predictions from the survey of specialists on North Korea at the start of the chapter – information can be a key tool for those seeking new methods with which to engage with or influence Pyongyang.

Aside from these research findings, the policy implications are also clear. In negotiations with the North, threats based on the economic or diplomatic tools of statecraft are less likely to impact the North's behavior or decision-making calculus than military exercises or information tools.

As with Russia, social media did not prove a fruitful area for current research. Future research on the North should continue to monitor social media for signs of increased use, but barring a sudden change by Pyongyang, official media websites rather than social media outlets are likely to remain the keys areas for data collection.

Based on the findings of the CSIS Beyond Parallel Project (that the North's reactions to military exercises are based on then current relations with the U.S.), a deeper examination of the timing of North Korean sentiment in response to the annual joint exercises may provide additional insights. However, the most important area for future research remains North Korean reaction(s) to the South's episodic use of loudspeakers along the border and any attempts by South Korean civic organizations to send leaflets over the border. A key for this research is determining whether and how Pyongyang adjusts to the information tools over time (as the regime has found success in doing when targeted with economic tools).

Chapter Six: Conclusion

In terms of both Russia and North Korea, this paper demonstrates the efficacy of information as a foreign policy tool at least on par with diplomatic, military, and economic tools – thus answering affirmatively the primary question posed at the outset. In both research chapters, information tools, in terms of both sentiment and actions/responses, produced a substantially stronger effect than diplomatic and economic tools, and in many cases produced a stronger effect than military tools.

The hypothesis that the more restrictive a state is of its domestic information environment, the more strongly it will react to the outside use of information tools, appears to have been met, but would benefit from further research. North Korea, dramatically more restrictive of its information environment than Russia, reacted more negatively than Russia to the outside use of information tools, both in terms of sentiment (all information-related terms for Pyongyang produced more negative sentiment than the terms used for Russia) and kinetic action. Whether there exists a comparative, sliding scale of negativity – that states like North Korea, most restrictive of their domestic information environment, react more negatively to outside information pressure than comparatively less restrictive states like Russia, would greatly benefit from the study of additional states. The author proposes Iran and China as the two most useful, policy-relevant candidates.

As noted, North Korea reacts more negatively to adversary military exercises than do the Russians. Investigating the reasons for this, along with any ties to specific IR approaches, also appears an interesting area for future research.

Finally, one additional point pertaining to deterrence in cyberspace. The demonstrated vulnerability of Russia and North Korea to information tools may offer an option for deterring and punishing cyberattacks. While more research is required, the idea of responding to a cyberattack from Pyongyang with leaflets, or from Moscow with criticism of the country's online censorship, may sound odd, but is supported by this research. A future paper focused on cyberspace, or a future examination of China using the framework here, may provide an opportunity to further develop this theory.

Technical Notes

Many of the findings here were based on sentiment analysis, an at-best inexact method for the automated evaluation and ranking of human communications. As anyone who has ever interacted with Apple's Siri, Amazon's Alexa, or similar systems can attest, machines and software can have difficulties understanding human communication. Sentiment analysis tools are no different. A future version of this research, with more capable or finely-tuned software may produce different results. However, in defense of the current software and methodology, any inaccuracies are unlikely to favor (i.e. be more or less accurate for) one foreign policy tool category over another – meaning, future research may refine the percentages, but is unlikely to change the respective ranking of the four categories.

Research using social media proved less fruitful than expected. The first issue was a limit on data access and collection – Twitter limiting most outside researchers

to the 3,200 most recent messages from an account instead of allowing access to all messages from an account. The second issue was data availability, including an apparent lack of interest in social media by the North Koreans. Both of these issues affected the ability of the research to fully and cogently examine all four categories of foreign policy tools. This may change in the future, if Twitter lifts the 3,200-tweet limit, Facebook grants greater access to researchers, or North Korea simply decides to engage more on social media. But all that would benefit future research, in terms of this paper, the level of insight gained from examining social media proved unsatisfactory.

The KCNA dataset, comprised of all English articles published by the organization from January 2002 to August 2017 (the cutoff point adopted in order to begin data analysis for this paper), provided the largest and most useful dataset. The datasets downloaded from the Russian Foreign Ministry and TASS were smaller, though targeted at specific topics. For future research, the preferred method would be that used for the KCNA – scrape all of the data/stories from the website, then analyze locally rather than searching on the websites and only downloading related articles.

Language limitations prevented deeper analysis of the targeted media organizations. The decision to use sentiment analysis, which allows for rapid analysis of tens of thousands of data points, enabled the research to incorporate much larger reporting datasets than would otherwise have been possible (for the KCNA, and thus North Korean state media reporting, it was essentially $N=\text{all}$ for the time period investigated). Unfortunately, sentiment analysis tools for Russian and

Korean are much less developed than those for English (at least in the commercial sector; select government organizations may have access to more robust, non-Western language analysis tools). While research in English is clearly capable of finding government sentiment in Russian and North Korean state media, and analysis of actions can occur regardless of language, future research with Russian and Korean capable sentiment analysis systems would likely prove beneficial.

As mentioned above, it is important to broaden our research scope to include additional countries, specifically China and Iran. Normally slotted between Russia and North Korea on rankings of freedom of the press or freedom of information access, these two countries appear the ripest for future research of the type conducted here. Which returns us to the point just raised – the research would likely have to occur in English until such time when capable sentiment analysis tools for Farsi and Chinese are commercially available.

At the outset of the paper, especially in the chapter on Russia, GDELT was expected to provide a key data resource. As research progressed however, the limitations of GDELT's data became apparent. In the North Korea chapter, GDELT's lack of collection from North Korean state media sources rendered it ineffective. Second, as mentioned in the Russia chapter, GDELT's focus on the military and diplomatic tools of statecraft, with few capabilities to classify and thereby examine information tools (even when incorporating 'cyber' as a proxy search/evaluation term), reduced GDELT's applicability for this research. Finally, GDELT is largely a mass ingestion and classification tool, which provides truly big data, but this becomes problematic when stories on Russia or North Korea appearing on media

outlets in, for example, Akron and Bangalore are given the same weight in the database as reports directly from sources in Pyongyang and Moscow. GDELT is an excellent method for taking the world's pulse on a topic, but (and this may simply be due to the limitations of this researcher) appears less effective for the state/official media focus of the research here.

Policy Recommendations

We began this research with several historical anecdotes, including one from the end of the Cold War on the key role played by the USIA in helping thwart a coup in the Soviet Union that helped launch the rule of a preferred U.S. candidate, Boris Yeltsin.²¹¹ The paper ends in a much different place, a period when Russia stands accused of using information tools to successfully alter the outcome of a U.S. election to launch the rule of its preferred candidate.

“During the Cold War, the U.S. Information Agency (USIA) conducted effective information operations against the Soviet Union,” and the failure to rebuild the organization, or have someone in charge of information operations, has cost the country.²¹² In the wake of Russia's interference in the U.S. election, the State Department's Global Engagement Center [GEC], started in March 2016 to counter terrorist (i.e. ISIS) messaging, was tasked with “attacking state-sponsored propaganda” under the Countering Foreign Propaganda and Disinformation Act,

²¹¹ This section is largely from Dizard, Wilson, *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pgs. 210-211.

²¹² Nagl, John A., “Knife Fights: A Memoir of Modern War in Theory and Practice”, pgs. 135-136.

signed into law by President Obama in December 2016.²¹³ The GEC's budget for 2017, \$36 million, compares to \$1.3 billion for the USIA in the mid-1990s (equivalent to just over \$2 billion in 2017 dollars).²¹⁴ ²¹⁵ While the DoD, intel agencies, and other parts of the government conduct information operations, the organization that helped coordinate and manage these activities from WWII until the late 1990s no longer exists, with few expectations that the GEC or a similar organization will come to fulfill this role anytime soon. Perhaps the only government organization with the funding and many (but not all) of the capabilities to fulfill this function, U.S. Cyber Command, is tasked and focused on a subset of the information environment, not the leaflets, loudspeakers, and other types of information tools examined and demonstrated effective here.

While this paper is not a call to restart the USIA, the turnaround in U.S. capabilities and strengths pre- and post-dissolution is stunning. This research has demonstrated that information remains a powerful tool for use against authoritarian states, but without the will and guidance to harness these tools they will continue to languish.

The chapter on North Korea found wide agreement across a spectrum of North Korea specialists on the importance of using information tools in negotiations or conflicts with the North. The South demonstrated the effectiveness of one of the tools, loudspeakers, in winning a rare expression of regret from the North over the landmine maiming of two soldiers. However, throughout recent attention on the

²¹³ Lapowsky, *The State Department's Fumbled Fight Against Russian Propaganda*, 2017.

²¹⁴ Lapowsky, *The State Department's Fumbled Fight Against Russian Propaganda*, 2017.

²¹⁵ Dizard, *Inventing Public Diplomacy: The Story of the U.S. Information Agency*, pg. 215.

North over its missile and nuclear programs, little mention has been made in the U.S. of using information as a tool to influence the North regarding these programs. Instead, discussions continue to focus on military, diplomatic, and economic responses of the same type used for decades.

While this researcher believes the North is as unlikely to give up its nuclear weapon and missile capabilities as the U.S., China, and Russia, outside efforts to influence the North regarding its program would likely benefit from adding information tools to the response kit. Simply stating a willingness to introduce into the North quantities of smartphones capable of accessing the outside world, then offering to forego that plan in exchange for influence over at least the scale and scope of the North's programs, costs literally nothing to announce and is, as demonstrated by this research, at least as likely to create gains as are the current foreign policy tools.

Policy options for Russia are similar. As demonstrated by the research above, NATO exercises, sanctions, and diplomatic efforts create less of a reaction from the Russian government, in terms of both sentiment and action, than does a focus on freedom of information access. Rather than the Cold War approach of infiltrating specific U.S. government themes and messages, an updated policy would need to focus on increased access and reduced censorship. A demonstration of the tools and will to operationalize such a policy would, based on the research above, result in greater influence over the Russian government than a continued focus on diplomatic, military, and economic tools.

In closing, this research has demonstrated the ability of information tools to affect the sentiment and actions, and thereby the decision-making calculus, of two authoritarian states. Further, it has shown that information was once a common, successful tool of U.S. foreign policy, but has become underutilized here at the dawn of the Information Age. Reincorporating information into the U.S. foreign policy toolkit, especially during interactions with authoritarian states, will produce cost-effective gains, especially at the outset as targeted regimes attempt to adjust to these possibly 'disruptive moves' (as described in the Communications theory section of the literature review). The capabilities, funding, history, and knowledge already exist, what remains lacking are the will, guidance, and imagination to use them.

Bibliography

Ackerman, Spencer. "U.S. Has Secret Tools to Force Internet on Dictators". *Wired*, 7 February 2011. <http://www.wired.com/dangerroom/2011/02/secret-tools-force-net/#more-40135>

Adams, James. "Virtual Defense." *Foreign Affairs*, no. May/June 2001 (May 1, 2001). <https://www.foreignaffairs.com/articles/2001-05-01/virtual-defense>, accessed 1 February 2017.

Adamson, Fiona. "Globalisation, Transnational Political Mobilisation, and Networks of Violence." *Cambridge Review of International Affairs*, October 2005.

Agence France-Presse. "S. Korea, US Begin Military Drill Despite N. Korea Threats." *Defense News*, August 19, 2015. <http://www.defensenews.com/story/defense/international/asia-pacific/2015/08/18/south-korea-us-begin-military-drill-despite-korea-threats/31928267/>.

Ahmann, Timothy, et al. "U.S. intelligence chief: China top suspect in government agency hacks", Reuters, 26 June 2015, <http://www.reuters.com/article/2015/06/26/us-cybersecurity-usa-china-idUSKBN0P525G20150626>. Accessed 14 October 2015.

American Marketing Association (AMA), *Definition of Marketing*, American Marketing Association Board of Directors, July 2013, AMA website, <https://www.ama.org/AboutAMA/Pages/Definition-of-Marketing.aspx>, accessed 11 July 2016.

Armistead, Leigh. *Information Operations Matters*. 1st ed. Washington, DC: Potomac Books, Inc., 2010.

Bae, Sebastian J. "Cyber Warfare: Chinese and Russian Lessons For US Cyber Doctrine - Georgetown Security Studies Review." *Georgetown Security Studies Review*, May 7, 2015. <http://georgetownsecuritystudiesreview.org/2015/05/07/cyber-warfare-chinese-and-russian-lessons-for-us-cyber-doctrine/>. Accessed 15 October 2015.

Baek, Jieun. *North Korea's Hidden Revolution: How the Information Underground Is Transforming a Closed Society*. New Haven: Yale University Press, 2016.

Bechtol, Bruce E. Jr., "Maintaining a Rogue Regime: Kim Jong-il and the North Korean Succession Process". *Korea Economic Institute Academic Paper Series*, Volume 4, Number 7, July 2009.

"Beyond Parallel." Beyond Parallel. Washington, DC: Center for Strategic and International Studies. <https://beyondparallel.csis.org/databases/>. Accessed 18 January 2018.

Berlo, David. *The Process of Communication: An Introduction to Theory and Practice*. Holt, Rinehart and Winston, 1960.

Boot, Max, and Michael Doran. "Political Warfare: Policy Innovation Memorandum." Council on Foreign Relations, June 28, 2013. <https://www.cfr.org/report/political-warfare>.

Breedlove, Philip, and Anders Fogh Rasmussen. "A NATO for a Dangerous World," August 18, 2014. Supreme Headquarters Allied Powers Europe. <http://www.shape.nato.int/a-nato-for-a-dangerous-world>. Accessed 22 January 2017.

Brodie, Bernard (1959), "8", *"The Anatomy of Deterrence" as found in Strategy in the Missile Age*, Princeton: Princeton University Press

Center for Nonproliferation Studies. "The CNS North Korea Missile Test Database." Monterey, CA: James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey, November 30, 2017. <http://www.nti.org/analysis/articles/cns-north-korea-missile-test-database/>. Accessed 20 December 2017.

Cha, Victor, Na Young Lee, and Andy Lim. "DPRK Provocations and US-ROK Military Exercises, 2005 to 2016." Beyond Parallel. Washington, DC: Center for Strategic and International Studies, August 18, 2016. <http://beyondparallel.csis.org/us-rok-exercises-not-provoke-dprk/>, accessed 18 March 2017.

Cha, Victor. *The Impossible State: North Korea, Past and Future*. HarperCollins, 2012.

Cheng, Dean. "The U.S. Needs an Integrated Approach to Counter China's Anti-Access/Area Denial Strategy." Background. Heritage Foundation, July 9, 2014. http://www.heritage.org/research/reports/2014/07/the-us-needs-an-integrated-approach-to-counter-chinas-anti-accessarea-denial-strategy#_ftn37. Accessed 21 October 2016.

Cheng, Dean. "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response." Background. Heritage Foundation, November 26, 2012. <http://www.heritage.org/research/reports/2012/11/winning-without-fighting-chinese-public-opinion-warfare-and-the-need-for-a-robust-american-response>. Accessed 21 October 2016.

China, People's Republic of; "Defense Policy," Ministry of National Defense, <http://eng.mod.gov.cn/Database/DefensePolicy/index.htm>. Accessed April 2, 2016.

Choe, Sang-hun. "Korean Navies Skirmish in Disputed Waters." *The New York Times*. November 10, 2009, online edition, sec. Asia Pacific. <http://www.nytimes.com/2009/11/11/world/asia/11korea.html>. Accessed 13 January 2018.

Choe, Sang-hun. "South Korea Bars Leaflet Drop Over Border With North." *The New York Times*, October 22, 2012. <http://www.nytimes.com/2012/10/23/world/asia/south-korea-bars-leaflet-drop-over-border-with-north.html>. Accessed 19 March 2016.

Choe, Sang-hun. "Computer Networks in South Korea Are Paralyzed in Cyberattacks." *The New York Times*, March 20, 2013. http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?_r=0, accessed 14 July 2016.

Choe, Sang-hun. "Koreas Exchange Fire After Activists Launch Balloons Over Border." *The New York Times*, October 10, 2014. <http://www.nytimes.com/2014/10/11/world/asia/koreas-exchange-fire-after-activists-launch-balloons-over-border.html>, accessed 19 March 2016.

Choe, Sang-hun. "Gunfire Exchanged across Korean Boundary." *The New York Times*. October 19, 2014, online edition, sec. Asia Pacific. <https://www.nytimes.com/2014/10/20/world/asia/gunfire-exchanged-on-korean-boundary.html>. Accessed 13 January 2018.

Choe, Sang-hun. "North Korea Placed Mines That Maimed Soldiers at DMZ, South Says." *The New York Times*, August 10, 2015. <http://www.nytimes.com/2015/08/11/world/asia/north-korea-placed-mines-that-maimed-2-south-korean-soldiers-at-dmz-seoul-says.html>. Accessed 10 August 2015.

Choe, Sang-hun. "South Korea Accuses the North After Land Mines Maim Two Soldiers in DMZ." *The New York Times*, August 10, 2015. <http://www.nytimes.com/2015/08/11/world/asia/north-korea-placed-mines-that-maimed-2-south-korean-soldiers-at-dmz-seoul-says.html>. Accessed 19 March 2016.

Choe, Sang-hun. "North Korea Denies It Laid Mines That Maimed Soldiers From South." *The New York Times*, August 14, 2015. <http://www.nytimes.com/2015/08/15/world/asia/north-korea-denies-it-laid-mines-that-maimed-soldiers-from-south.html>. Accessed 15 August 2015.

Choe, Sang-hun. "North and South Korea Trade Fire Across Border, Seoul Says." *The New York Times*, August 20, 2015.

<http://www.nytimes.com/2015/08/21/world/asia/north-korea-and-south-korea-exchange-rocket-and-artillery-fire.html>. Accessed 20 August 2015.

Choucrist, Nazli. "Introduction: CyberPolitics in International Relations." *International Political Science Review* 21, no. 3 (July 2000): 243–63.

Choucrist, Nazli. *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press, 2012.

Choucrist, Nazli, and David Clark. "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma." In *Explorations in Cyber International Relations*, Vol. Working Paper No. 2012-- - 29. MIT Political Science, 2012.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2178586, accessed 3 February 2017.

Clapper, James. Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee. Washington, DC, 2016.

https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf, accessed 12 July 2016.

CNN, "Koreas Agree to Military Hotline." News. CNN, June 4, 2004.

<http://www.cnn.com/2004/WORLD/asiapcf/06/03/koreas.agree/index.html>. Accessed 13 January 2018.

Cohen, Noam. "Hong Kong Protests Propel FireChat Phone-to-Phone App", *The New York Times*, 5 October 2014,

<http://www.nytimes.com/2014/10/06/technology/hong-kong-protests-propel-a-phone-to-phone-app.html? r=0>, accessed 22 May 2016.

Coll, Steve. "Ghost Wars". New York: *Penguin Books*, 2004.

Connell, Michael. "Iran's Military Doctrine." *The Iran Primer*, United States Institute of Peace. Accessed April 3, 2016. <http://iranprimer.usip.org/resource/irans-military-doctrine>, accessed 3 April 2016.

Corman, Steven R., Angela Trethewey, and Bud Goodall. "A 21st Century Model for Communication in the Global War of Ideas." *Consortium for Strategic Communication*, no. 701 (April 3, 2007): 1–18.

Cornell University Library, *The January 25 Revolution, Arab Spring: A Research & Study Guide*, Cornell University, May 2016,

<http://guides.library.cornell.edu/c.php?g=31688&p=200748>, accessed 21 May 2016.

Cornish, Paul; Livingstone, David; Clemente, Dave; Yorke, Claire. "On Cyber Warfare: A Chatham House Report". *Chatham House*, November 2010.

Crawford, Kate. "Think Again: Big Data." *Foreign Policy*, May 10, 2013. <https://foreignpolicy.com/2013/05/10/think-again-big-data/>. Accessed 12 February 2016.

Crocker, Lizzie. "North Korea's Secret Movie Bootleggers: How Western Films Make It Into the Hermit Kingdom." *The Daily Beast*, December 22, 2014. <http://www.thedailybeast.com/articles/2014/12/22/north-korea-s-secret-movie-bootleggers-how-western-films-make-it-into-the-hermit-kingdom.html>. Accessed 3 August 2015.

Cronin, Audrey Kurth. "Cyber-Mobilization: The New Levee en Masse". *Parameters*, summer 2006.

Cukier, Kenneth Neil, and Viktor Mayer-Schoenberger. "The Rise of Big Data How It's Changing the Way We Think About the World." *Foreign Affairs* 92, no. May/June 2013 (April 3, 2013): 28–40.

Daniels, Laura. "RUSSIAN ACTIVE MEASURES IN GERMANY AND THE UNITED STATES: ANALOG LESSONS FROM THE COLD WAR." *War on the Rocks*, September 27, 2017. <https://warontherocks.com/2017/09/russian-active-measures-in-germany-and-the-united-states-analog-lessons-from-the-cold-war/>, accessed 28 September 2017.

Davenport, Kelsey. "UN Security Council Resolutions on North Korea." Washington, DC: Arms Control Association, October 2017. <https://www.armscontrol.org/factsheets/UN-Security-Council-Resolutions-on-North-Korea>. Accessed 20 December 2017.

Davis, Julie Hirschfeld. "U.S. Imposes Sanctions Over Russia's Intervention in Ukraine." *The New York Times*, December 22, 2015. <http://www.nytimes.com/2015/12/23/world/europe/us-russia-ukraine-sanctions.html>, accessed 19 March 2016.

Davis, Julie Hirschfeld. "Hacking of Government Computers Exposed 21.5 Million People." *The New York Times*. July 9, 2005. <http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html? r=0>, accessed 3 August 2016.

Department of State, Bureau of Public Affairs. "Human Rights Reports." Government organization, 2015. <http://www.state.gov/j/drl/rls/hrrpt/>. Accessed 20 March 2016.

Department of State, Department of Treasury. *Ukraine and Russia Sanctions. Executive Order 13660*. Vol. 13660, 2014.
<http://www.state.gov/e/eb/tfs/spi/ukrainerrussia/>. Accessed 19 March 2016.

Denning, Dorothy E. "Information Warfare and Security". New York: *ACM Press Books*, 1999.

"Department of Defense 2015 Cyber Strategy." Department of Defense, April 2015.
http://www.defense.gov/home/features/2015/0415_cyber-strategy/. Accessed 3 August 2015.

Dizard, Wilson. *Inventing Public Diplomacy: The Story of the U.S. Information Agency*. Boulder and London: Lynne Rienner Publishers, 2004.
Drezner, Daniel. "The Global Governance of the Internet: Bringing the State Back In." *Political Science Quarterly* 119 (2004): 477–98.

Dunn, Alexandra. "Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising." The Fletcher Forum on World Affairs, The Fletcher School, Tufts University, 15 May 2011. <http://www.fletcherforum.org/2011/05/15/dunn/>, accessed 21 May 2016.

Elder, Robert E. *Information Machine: The United States Information Agency and American Foreign Policy*. 1st ed. Syracuse University Press, 1968.

Emmott, Robin. "As Russia Reasserts Itself, NATO Opens Biggest Exercises in Years." *Reuters*, October 19, 2015. <http://www.reuters.com/article/us-nato-exercises-idUSKCN0SD1F920151019>. Accessed 19 March 2016.

Eriksson, Johan, and Giampiero Giacomello. "The Information Revolution, Security, and International Relations: (IR)relevant Theory?" *International Political Science Review* 27, no. 3 (July 2006): 221–44.

EU. "EU Sanctions against Russia over Ukraine Crisis." European Union, March 2014.
http://europa.eu/newsroom/highlights/special-coverage/eu_sanctions/index_en.htm. Accessed 19 March 19, 2016.

Everard, John. *Only Beautiful, Please: A British Diplomat in North Korea*. Stanford University: The Walter H. Shorenstein Asia-Pacific Research Center, 2012.

Fifield, Anna. "S. Korea Agrees to End Broadcasts as North Expresses Regret for Provocations." *Washington Post*. August 24, 2015, online edition, sec. Asia & Pacific.
https://www.washingtonpost.com/world/asia_pacific/north-korea-hates-those-loudspeakers-because-they-make-fun-of-kim/2015/08/24/439f6039-3f37-490b-9fa1-e3b8022893e6_story.html?utm_term=.22ecaee52e73. Accessed 13 January 13, 2018.

Fifield, Anna. "U.S. Planning to Press Harder against North Korea on Human Rights." *Washington Post*, July 26, 2015.

https://www.washingtonpost.com/world/asia_pacific/us-plans-to-press-north-korea-harder-on-human-rights/2015/07/26/10c5ff32-2f0a-11e5-818f-a242f28e7022_story.html?tid=hybrid_collaborative_1_na. Accessed 3 August 2015.

Fink, Naureen Chowdhury and Barclay, Kack. "Mastering the Narrative Counterterrorism Strategic Communication and the United Nations", Center on Global Counterterrorism Cooperation, February 2013, http://www.globalcenter.org/wp-content/uploads/2013/03/Feb2013_CT_StratComm.pdf. Accessed 15 October 2015.

Freedom House. "Freedom in the World 2017." Washington, DC: Freedom House, 2017. <https://freedomhouse.org/report/freedom-world/freedom-world-2017#anchor-one>. Accessed 17 December 2017.

Freedom House. "Freedom of the Press 2017: Press Freedom's Dark Horizon." Washington, DC: Freedom House, 2017. <https://freedomhouse.org/report/freedom-press/freedom-press-2017>. Accessed 17 December 2017.

Freedom House. "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy." Washington, DC: Freedom House, 2017. <https://freedomhouse.org/report/freedom-net/freedom-net-2017>. Accessed 22 April 2018.

Freedom House, *Reports*, <https://freedomhouse.org/reports>, accessed 29 January 2017.

GAO. "Cybersecurity." U.S. Government Accountability Office (GAO), 2015. http://www.gao.gov/key_issues/cybersecurity/issue_summary, accessed 13 July 2016.

"GDELT CAMEO: Conflict and Mediation Event Observations; Event and Actor Codebook." Department of Political Science, Pennsylvania State University, March 2012. <http://eventdata.psu.edu/>.

GDELT Project, GDELT project website, <http://www.gdeltproject.org>, accessed 16 October 2016.

GDELT Project, "GDELT – DATA FORMAT CODEBOOK V 1.03." GDELT Project, August 25, 2013. <http://data.gdeltproject.org/documentation/GDELT-Data Format Codebook.pdf>, accessed 16 October 2016.

Gerasimov, Valery. "The Value of Science in Prediction." *Military-Industrial Kurier*, February 27, 2013.

Gilboa, Eytan, Maria Gabrielsen Jumbert, Jason Miklian, and Piers Robinson. "Moving Media and Conflict Studies Beyond the CNN Effect." *Review of International Studies*, March 2016, 1–19. doi:10.1017/S026021051600005X.

Gjeltén, Tom. "Seeing The Internet As An 'Information Weapon.'" NPR, September 23, 2010. <http://www.npr.org/templates/story/story.php?storyId=130052701>, accessed 14 December 2016.

Gompert, David C. and Hans Binnendijk. *The Power to Coerce: Countering Adversaries Without Going to War*. Santa Monica, CA: RAND Corporation, 2016. http://www.rand.org/pubs/research_reports/RR1000.html, accessed 15 July 2016.

Groll, Elias. "White House: The Internet May Be a Strategic Liability to the West." *Foreign Policy*, February 11, 2016. <https://foreignpolicy.com/2016/02/11/white-house-the-internet-may-be-a-strategic-liability-to-the-west/>. Accessed 12 February 2016.

Gustin, Sam. "Social Media Sparked, Accelerated Egypt's Revolutionary Fire," *Wired Business*, 11 February, 2011, <http://www.wired.com/2011/02/egypts-revolutionary-fire/>, accessed 21 May 2016.

Haggard, Stephan, and Marcus Noland. "North Korea's Foreign Economic Relations." *International Relations of the Asia-Pacific* 8, no. 2 (May 1, 2008): 219–46. doi:10.1093/irap/lcn005.

Haggard, Stephan and Noland, Marcus. "Political Attitudes under Repression - Evidence from North Korean Refugees". *East-West Center Working Papers*, No. 21, March, 2010. <http://www.eastwestcenter.org/fileadmin/stored/pdfs/pswp021.pdf>

Haggard, Stephan, and Marcus Noland. *Witness to Transformation: Refugee Insights into North Korea*. Washington, DC: Peterson Institute for International Economics, 2011.

Harden, Blaine. "Resistance against N. Korean regime taking root, survey suggests." *Washington Post*, 24 March 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/03/23/AR2010032304035.html?wprss=rss_world

Harding, Luke. "Russia Threatening New Cold War over Missile Defence." *The Guardian*, April 11, 2007, sec. World news. <http://www.theguardian.com/world/2007/apr/11/usa.topstories3>. Accessed 20 March 2016.

Heintz, Andy. "In the Nuclear Standoff, Ordinary North Koreans Disappear." Interview with an expert. Washington, DC: Institute for Policy Studies, January 8,

2018. <http://fpif.org/nuclear-standoff-ordinary-north-koreans-disappear/>. Accessed 13 January 2018.

Henderson, Simon. "The 'al-Jazeera Effect': Arab Satellite Television and Public Opinion." Policy Analysis. Policywatch. Washington, DC: *The Washington Institute for Near East Policy*, December 8, 2000. <http://www.washingtoninstitute.org/policy-analysis/view/the-al-jazeera-effect-arab-satellite-television-and-public-opinion>, accessed 2 August 2017.

Herman, Edward S., and Noam Chomsky. *Manufacturing Consent: The Political Economy of the Mass Media*. New York: Pantheon Books, 1988.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60. DOI: <http://dx.doi.org/10.5038/1944-0472.4.2.3>, available at: <http://scholarcommons.usf.edu/jss/vol4/iss2/4>, accessed 14 July 2016.

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4, no. 2 (2011): 1-24. DOI: <http://dx.doi.org/10.5038/1944-0472.4.2.1>, available at: <http://scholarcommons.usf.edu/jss/vol4/iss2/2>, accessed 14 July 2016.

Hwan, Kim Seong. "Radio Can Help Kickstart a Revolution, North Koreans Say." *The Guardian*, September 21, 2015, <http://www.theguardian.com/world/2015/sep/21/north-korea-radio-broadcasts-bbc-kim-jong-un-regime>. Accessed 15 October 2015.

International Crisis Group. "North Korea under Tightening Sanctions". *Crisis Group Asia Briefing N°101*. 15 March 2010.

Jeong Rak-in. "There is no DMZ blocking cellphones". *Sisa Journal*, 16 February 2011. <http://www.sisapress.com/news/articleView.html?idxno=54396>. Translation by author.

Jeong Rak-in. "Defector Broker: Managing 200 People". *Sisa Journal*, 16 February 2011. <http://www.sisapress.com/news/articleView.html?idxno=54392#>. Translation by author.

Jervis, Robert, Richard N. Lebow and Janice G. Stein. 1985. *The Psychology of Deterrence*. Baltimore: Johns Hopkins University Press.

Jung, Jin-Heon. "Ballooning Evangelism: Psychological Warfare and Christianity in the Divided Korea." MMG Working Paper 14-07. Göttingen, Germany: Max-Planck-Institute for the Study of Religions and Ethnic Diversity, 2014. http://www.mmg.mpg.de/fileadmin/user_upload/documents/wp/WP_14-07_Jung%20Ballooning%20Evangelism.pdf. Accessed 12 January 2018.

Karimi, Faith, and Jungeun Kim. "N. Korea Retaliates, Broadcasts Propaganda into South." CNN. Accessed August 17, 2015.

<http://www.cnn.com/2015/08/17/asia/north-korea-propaganda-broadcasts/index.html>. Accessed 15 October 2015.

Kay, Sean. "Globalization, Power, and Security." *Security Dialog*, Vol. 35, No. 1 (2004).

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017.

Kennan, George. "The Long Telegram: The Charge in the Soviet Union (Kennan) to the Secretary of State." Telegram. Moscow: U.S. Department of State, February 22, 1946. <http://nsarchive2.gwu.edu/coldwar/documents/episode-1/kennan.htm>. Accessed 29 September 2017.

Kennan, George. "The Inauguration of Organized Political Warfare." U.S. Department of State, April 30, 1948. Wilson Center. <https://digitalarchive.wilsoncenter.org/document/114320>.

Keohane, Robert O. and Martin, Lisa L. "The Promise of Institutionalist Theory." *International Security*, Vol. 20 No. 1 (Summer 1995).

Kirsch, Adam. "Technology Is Taking Over English Departments: The False Promise of the Digital Humanities." *New Republic*, May 2, 2014. <https://newrepublic.com/article/117428/limits-digital-humanities-adam-kirsch>, accessed 8 January 2017.

Kim, Christine. "Seoul to crank up DMZ propaganda". *JoongAng Daily*, 6 October 2010. <http://joongangdaily.joins.com/article/view.asp?aid=2926810>

Kirk, Donald. "Kim Jong-il birthday: North watches tributes, South sends propaganda balloons". *The Christian Science Monitor*, 16 February 2011. <http://www.csmonitor.com/World/Asia-Pacific/2011/0216/Kim-Jong-il-birthday-North-watches-tributes-South-sends-propaganda-balloons>

Klimentyev, Michael. "Russia's National Security Strategy for 2016 in 9 Key Points." *RT*, December 31, 2015. <https://www.rt.com/news/327608-russia-national-security-strategy/>, accessed 3 April 2016.

Klug, Foster. "North Korea Threatens Strikes over S. Korean Propaganda Broadcasts, Denies Role in Mine Blasts." *US News & World Report*. <http://www.usnews.com/news/world/articles/2015/08/14/n-korea-threatens-strikes-over-skorea-propaganda-broadcasts>. Accessed August 17, 2015.

Knepper, William E. "Soviet Active Measures." presented at the Chicago Council on Foreign Relations, Chicago, May 30, 1984.
<https://archive.org/stream/departmentofstatc1984unit/departmentofstatc1984unit.djvu.txt>. Accessed 29 September 2017.

Korayem, Mohammed, Khalifeh Aljadda, and David Crandall.
"Sentiment/Subjectivity Analysis Survey for Languages Other than English." School of Informatics and Computing, Indiana University; CareerBuilder, August 26, 2016.
<https://arxiv.org/pdf/1601.00087.pdf>. Accessed August 31, 2017.

Kramer, Andrew. "NATO Ships Cause Alarm in Moscow Alliance Raises Its Profile in Black Sea." *International Herald Tribune*, August 27, 2008, Europe edition.
<https://web.archive.org/web/20080831044219/http://www.ihf.com/articles/2008/08/27/europe/georgia.php>.

Kretchun, Nat, Catherine Lee, and Seamus Tuohy. 2017. "Compromising Connectivity: Information Dynamics Between the State and Society in a Digitizing North Korea." Washington, DC: Intermedia. <http://www.intermedia.org/8044-2/>.

Lankov, Andrei. *North of the DMZ*. McFarland and Company, Inc., Jefferson, North Carolina, 2007.

Lankov, Andrei. *The Real North Korea: Life and Politics in the Failed Stalinist Utopia*. Oxford University Press, 2013.

Lankov, Andrei. "Changing North Korea." *Foreign Affairs*, November/December 2009 (2009). <https://www.foreignaffairs.com/articles/asia/2009-11-01/changing-north-korea>. Accessed 1 August 2015.

Lapowsky, Issie. "The State Department's Fumbled Fight Against Russian Propaganda." *Wired*, November 22, 2017, online edition, sec. Security.
<https://www.wired.com/story/the-state-departments-fumbled-fight-against-russian-propaganda/>. Accessed 14 January 2018.

Lee Young-jong and Kim, Christine. "In North, not a peep about revolution in Egypt". *JoongAng Daily*, 16 February 2011.
<http://joongangdaily.joins.com/article/view.asp?aid=2932267>. Accessed 20 March 2016.

Leetaru, Kalev H. "Culturomics 2.0: Forecasting Large-scale Human Behavior Using Global News Media Tone in Time and Space." *First Monday* 16, no. 9 (September 5, 2011). <http://firstmonday.org/ojs/index.php/fm/article/view/3663/3040>, accessed 18 August 2016.

Lilly, Bilyana. "How Putin Uses Missile Defence in Europe to Distract Russian Voters." *NATO Review Magazine*, 2015.

<http://www.nato.int/docu/review/2015/Russia/Ballistic-Missile-Defence-Putin/EN/index.htm>. Accessed 20 March 2016.

Litwak, Robert S., *Regime Change*. Woodrow Wilson Center Press, Washington, DC, 2007.

Lohr, Steve. "Ideas & Trends: Net Americana; Welcome to the Internet, The First Global Colony." *The New York Times*. January 9, 2000.
<http://www.nytimes.com/2000/01/09/weekinreview/ideas-trends-net-americana-welcome-to-the-internet-the-first-global-colony.html>, accessed 2 August 2016.

Lydia/TextMap Publications, Stony Brook University website,
<http://www3.cs.stonybrook.edu/~skiena/lydia/>, accessed 7 February 2016.

Marinos, Louis, Adrian Belmonte, and Evangelos Rekleitis. "European Union Agency For Network And Information Security (ENISA) Threat Landscape 2015." European Union Agency For Network And Information Security, January 2016.
<https://www.enisa.europa.eu/publications/etl2015>, accessed 14 July 2016.

Manyin, Mark E. and Nikitin, Mary Beth. "U.S. Assistance to North Korea". *CRS Report for Congress* (Order Code RS21834), 31 July 2008.

McDonald, Mark. "N. Korea Threatens South on Balloon Propaganda". *The New York Times*, 27 February 2011.
<http://www.nytimes.com/2011/02/28/world/asia/28korea-balloons.html>

McEachern, Patrick. *Inside the Red Box: North Korea's Post-Totalitarian Politics*. New York, New York: Columbia University Press, 2010.

MeaningCloud. "What Is Sentiment Analysis?" MeaningCloud LLC, 2018.
<https://www.meaningcloud.com/developer/sentiment-analysis/doc/2.1/what-is-sentiment-analysis>.

Media Center, Media Center website (<https://sources.mediameter.org>), Berkman Center for Internet & Society at Harvard University and the Center for Civic Media at MIT, accessed 14 February 2016.

Merriam-Webster's Learner's Dictionary, Full Definition of marketing, Merriam-Webster, <http://www.merriam-webster.com/dictionary/marketing>, accessed 11 July 2016.

Mia. "Editor's Choice: Sentiment Analysis Is Opinion Turned into Code." Professional/Academic. Digital Humanities Now, April 7, 2015.
<http://digitalhumanitiesnow.org/2015/04/editors-choice-sentiment-analysis-is-opinion-turned-into-code/>, accessed 8 January 2017.

Mullen, Jethro, and Kathy Novak. "South Korea: Propaganda Broadcasts at North to Resume - CNN.com." CNN. Accessed August 10, 2015.

<http://www.cnn.com/2015/08/09/asia/koreas-tensions/index.html>.

Myers, B. R., *The Cleanest Race: How North Koreans See Themselves--And Why It Matters*. New York: Melville House, 2010.

Nagl, John A., "Knife Fights: A Memoir of Modern War in Theory and Practice", Penguin Press, New York, 2014.

NATO. "AJP-3.10 Allied Joint Doctrine for Information Operations." NATO Standardization Agency, November 2009. <https://info.publicintelligence.net/NATO-IO.pdf>, accessed 15 July 2016.

NATO. "History of NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia." Government organization. *CCDCOE*, May 23, 2014. <https://www.ccdcoe.org/history>. Accessed 20 March 2016.

NATO. "NATO Military Public Affairs Policy." NATO Headquarters, February 2011. <http://www.nato.int/ims/docu/mil-pol-pub-affairs-en.pdf>, accessed 15 July 2016.

NATO. "NATO Opens New Centre of Excellence on Cyber Defence." NATO, May 14, 2008. <http://www.nato.int/docu/update/2008/05-may/e0514a.html>. Accessed 20 March 2016.

NATO. "Statement by the North Atlantic Council on the Russian Recognition of South Ossetia and Abkhazia Regions of Georgia." NATO North Atlantic Council, August 27, 2008. <http://www.nato.int/docu/pr/2008/p08-108e.html>. Accessed 19 March 2016.

NATO Strategic Communications Centre of Excellence (NATO StratCom COE), *About Strategic Communications*, <http://www.stratcomcoe.org/about-strategic-communications>, accessed 13 July 2016.

Newmyer, Jacqueline. "The Revolution in Military Affairs with Chinese Characteristics." *Journal of Strategic Studies* 33:4 (August 20, 2010). doi:10.1080/01402390.2010.48970. <http://dx.doi.org/10.1080/01402390.2010.489706>, accessed 11 February 2017.

Niksch, Larry. "Korea: U.S.-Korean Relations — Issues for Congress." Congressional Research Service, June 16, 2005. <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjIutve6b7LAhWFsh4KHARrBCkQFgggMAE&url=https%3A%2F%2Fwww.fas.org%2Fsgp%2Fcrs%2Frow%2FIB98045.pdf&usg=AFQjCNG9PBQT>

[1m5pc24Guf8gGgqKYp00dg&sig2=xfZQdgrpp03cnQvLPWBpjQ&bvm=bv.116636494,d.dmo](#); accessed 20 March 2016.

NKchosun.com, [No author provided]. "North Korea Warns Defector Organizations". *NKchosun.com*, 23 March 2010.
http://nk.chosun.com/news/news.html?ACT=detail&res_id=123815. Translation by author.

NKeconwatch.com, *DPRK's Linux OS: Red Star*, 1 March 2010.
<http://www.nkeconwatch.com/2010/04/06/dprks-linux-os-red-star/>

Noland, Marcus. "They're Not Brainwashed, They're Just Miserable." *Foreign Policy Magazine*, 30 March 2010.
http://www.foreignpolicy.com/articles/2010/03/30/theyre_not_brainwashed_the_yre_just_miserable?page=0,1

Noland, Marcus. "Avoiding the Apocalypse: The Future of the Two Koreas". *Institute for International Economics*, June 2000.

Nye, Jr., Joseph S. "Soft Power: The Means to Success in World Politics." 1st ed. New York, NY: Public Affairs, 2004.

Nye, Jr., Joseph S. "Think Again: Soft Power." *Foreign Policy*, February 23, 2006.
<http://foreignpolicy.com/2006/02/23/think-again-soft-power/>. Accessed 23 October 2016.

Nye, Jr., Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. No. 3 (Winter 2016/17) (2017): 44–71. doi:10.1162/ISEC_a_00266.

Obama, Barak, "Executive Order 13584 --Developing an Integrated Strategic Counterterrorism Communications Initiative", Office of the Press Secretary, The White House, 9 September 2011, <http://www.whitehouse.gov/the-press-office/2011/09/09/executive-order-13584-developing-integrated-strategic-counterterrorism-c>.

Obama, Barack. "National Security Strategy 2015." The White House, February 2015.
https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf, accessed 13 July, 2016.

Oliker, Olga. "Unpacking Russia's New National Security Strategy." Washington, DC: Center for Strategic and International Studies, January 7, 2016.
<http://csis.org/publication/unpacking-russias-new-national-security-strategy>, accessed 2 April 2016.

Open Radio for North Korea [no author provided]. "The Person behind the North's Cyberwar is Kim Jong-eun". *NKradio.org*, 8 March 2011.
<http://www.nkradio.org/news/5674>. Translation by author.

Pang, Bo, and Lillian Lee. "Opinion Mining and Sentiment Analysis." *Foundations and Trends in Information Retrieval* 2, no. No 1-2 (2008) (2008): 1-135.

Park, Ju-Min, and Tony Munroe. "North, South Korea Reach Agreement to Ease Tensions." *Reuters*, August 25, 2015.
<http://www.reuters.com/article/2015/08/25/us-northkorea-southkorea-idUSKCN0QR02D20150825>.

Person, James, et. al. "Crisis and Confrontation on the Korean Peninsula: 1968-1969". *North Korea International Documentation Project*, Woodrow Wilson Center, September 2008.
http://www.wilsoncenter.org/index.cfm?topic_id=230972&fuseaction=topics.publications&doc_id=474527&group_id=474507.

Pollack, Jonathan D.. "The Strategic Futures and Military Capabilities of the Two Koreas". *Strategic Asia*, 2005-06.

Pollack, Jonathan, "Kim Jong-il's Clenched Fist." *The Washington Quarterly*, October 2009.

Powell, Jon T. "Towards a Negotiable Definition of Propaganda for International Agreements Related to Direct Broadcast Satellites." *Law and Contemporary Problems* 45, no. 1 (Winter 1982): 3-35.

Pritchard, Charles L. and Tilelli, John H. Jr., "U.S. Policy Toward the Korean Peninsula". *Council on Foreign Relations*, 2010.

Puddington, Arch, and Tyler Roylance. "Anxious Dictators, Wavering Democracies: Global Freedom under Pressure, FREEDOM IN THE WORLD 2016." Washington, DC: Freedom House, 2016.
https://freedomhouse.org/sites/default/files/FH_FITW_Report_2016.pdf, accessed 13 July 2016.

Puddington, Arch. *Breaking Down Democracy: Goals, Strategies, and Methods of Modern Authoritarians*. Freedom House, June 2017,
https://freedomhouse.org/sites/default/files/June2017_FH_Report_Breaking_Down_Democracy.pdf. Accessed 21 April 2018.

Puddington, Arch, and Tyler Roylance. "Freedom in the World 2017 - Populists and Autocrats: The Dual Threat to Global Democracy." Washington, DC: Freedom House, 2017. <https://freedomhouse.org/report/freedom-world/freedom-world-2017#anchor-one>. Accessed 17 December 2017.

Raustiala, Kal. "An Internet Whole and Free: Why Washington Was Right to Give Up Control." *Foreign Affairs*, no. March/April 2017 (March 2017): 140–47, <https://www.foreignaffairs.com/articles/world/2017-02-13/internet-whole-and-free>, accessed 30 March 2017.

Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." presented at the 2012 ISA Annual Convention, San Diego, CA, April 1, 2012. [http://ecir.mit.edu/images/stories/Reardon%20and%20Choucri ISA 2012.pdf](http://ecir.mit.edu/images/stories/Reardon%20and%20Choucri%20ISA%202012.pdf), accessed 31 January 2017.

Reporters Without Borders. "2017 World Press Freedom Index." Paris: Reporters Without Borders, 2017. <https://rsf.org/en/ranking>. Accessed 16 December 2017.

Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 4–37. doi:10.1080/01402390.2014.977382.

Robinson, Linda, Todd Helmus, Raphael Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva. "Modern Political Warfare: Current Practices and Possible Responses." Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR1772.html.

Roosevelt, Franklin D: "Executive Order 9182 Establishing the Office of War Information,," June 13, 1942. Online by Gerhard Peters and John T. Woolley, *The American Presidency Project*. <http://www.presidency.ucsb.edu/ws/?pid=16273>, accessed 25 July 2016.

Runkle, Benjamin. "The Best Strategy for Cyber-Conflict May Not Be a Cyber-Strategy." War on the Rocks, November 8, 2016. <http://warontherocks.com/2016/11/the-best-strategy-for-cyber-conflict-may-not-be-a-cyber-strategy/>, accessed 14 December 2016.

Sanger, David. "U.S. Decides to Retaliate Against China's Hacking." *The New York Times*, July 31, 2015. http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0

Schelling, T. C. (1966), *The Diplomacy of Violence*, New Haven: Yale University Press

Schmidt, Eric, and Cohen, Jared. "The Digital Disruption: Connectivity and the Diffusion of Power." *Foreign Affairs*, no. November/December 2010 (November 1, 2010). <https://www.foreignaffairs.com/articles/2010-10-16/digital-disruption>, accessed 31 January 2017.

Schmitt, Michael, Liis Vihul, and NATO Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual 2.0 on the International Law Applicable to Cyber*

Operations. 2.0. Estonia: Cambridge University Press, 2017.
<https://ccdcoe.org/tallinn-manual.html>, accessed 7 November 2017.

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*. Indianapolis, IN: Wiley Publishing Inc., 2000.

Security Council Report. "UN Documents for DPRK (North Korea)." New York, NY: Security Council Report, September 2017.
<http://www.securitycouncilreport.org/un-documents/dprk-north-korea/>. Accessed 20 December 2017.

Seib, Phillip. *The Al Jazeera Effect: How the New Global Media Are Reshaping World Politics*. Lincoln: University of Nebraska Press, 2011.

Shannon, Claude E., and Warren Weaver. *The Mathematical Theory of Communication*. Tenth Printing, 1964. Urbana: The University of Illinois Press, 1964.

Shirky, Clay. "The Political Power of Social Media". *Foreign Affairs*, January/February 2011.

Siboni, Gabi, and Sami Kronenfeld. "Iran's Cyber Warfare." INSS Insight. Tel Aviv, Israel: The Institute for National Security Studies, October 15, 2012.
<http://www.inss.org.il/index.aspx?id=4538&articleid=5203>, accessed 3 April 2016.

Skipnichuk, Alexander. "Exercise Saber Guardian Joins Rapid Trident in Ukraine." U.S. Army, July 28, 2015. <http://www.army.mil/article/152937/>. Accessed 20 March 2016.

South Korea, Ministry of Unification. "Inter-Korean Exchanges and Cooperation." Major Statistics in Inter-Korean Relations. Seoul, Korea: Ministry of Unification, 2015.
http://unikorea.go.kr/download.do?filename=42602_201504011309360471.pdf.

South Korea, Ministry of Unification. "Inter-Korean Exchanges of People and Goods." Major Statistics in Inter-Korean Relations. Seoul, Korea: Ministry of Unification, 2015.
http://unikorea.go.kr/download.do?filename=42602_201504011309360482.pdf.

"Soviet Active Measures: Forgery, Disinformation, Political Operations." Washington, DC: U.S. Department of State, *Bureau of Public Affairs*, October 1981.
<http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20Forgery,%20Disinformation,%20Political%20Operations%20October%201981.pdf>, accessed 29 September 2017.

"SOVIET ACTIVE MEASURES IN THE ERA OF GLASNOST: A Report to Congress by the United States Information Agency." Report to Congress. Washington, DC: U.S.

Information Agency, March 1988. [InsidetheColdWar.org](http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20in%20the%20Era%20of%20Glasnot%20March%201988.pdf).
<http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20in%20the%20Era%20of%20Glasnot%20March%201988.pdf>.
Accessed 29 September 2017.

Snyder, Alvin. *Warriors of Disinformation: American Propaganda, Soviet Lies, and the Winning of the Cold War, An Insider's Account*. 1st ed. New York: Arcade Publishing, 1997.

Snyder, Scott. "What's Driving Pyongyang?". *The Oriental Economist*, July 2009.

Soldatov, Andrei, and Irina Borogan. *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*. 1st ed. New York: PublicAffairs, a member of the Perseus Book Group, 2015.

South Korean Ministry of Unification, "Inter-Korean Affairs, Humanitarian Cooperation, Humanitarian Assistance, Aid to North Korea".
http://eng.unikorea.go.kr/eng/default.jsp?pgname=AFFhumanitarian_assistance.

Sprague, Mansfield. "Report of the President's Commission on Information Activities Abroad." Department of State Bulletin. Department of State, February 8, 1961.
https://archive.org/stream/departmentofstat441961unit/departmentofstat441961unit_djvu.txt, accessed 1 August 2016.

Stavridis, James. "How to Win the Cyberwar Against Russia." *Foreign Policy*, October 12, 2016. <https://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/>, accessed 14 December 2016.

Stengel, Richard; "Under Secretary for Public Diplomacy and Public Affairs", The State Department, <http://www.state.gov/r/>.

Stevens, Tim. "Breaching Protocol: The Threat of Cyberespionage." *Jane's Intelligence Review* 22, no. 3 (2010): 8–13.

Svetoka, Sanda, and Anna Reynolds. *Social Media as a Tool of Hybrid Warfare*. Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2016.

Tatham, Steve. "U.S. GOVERNMENTAL INFORMATION OPERATIONS AND STRATEGIC COMMUNICATIONS: A DISCREDITED TOOL OR USER FAILURE? IMPLICATIONS FOR FUTURE CONFLICT." United States Army War College Press, December 2013.

Taylor, Philip M. "Munitions of the Mind". Third Edition. Manchester University Press, 2003. Also see the Second Edition, 1995.

Thornton, Rod. "Asymmetric Warfare". *Polity Press*, Cambridge, UK, 2007.

Tilghman, Andrew. "Military Exercise in South Korea Resumes amid Tensions." *MilitaryTimes*, August 21, 2015.

<http://www.militarytimes.com/story/military/2015/08/21/korea-tension-exercise/32120565/>. Accessed 19 March 2016.

UN, "Charter of the United Nations." 1 UNTS XVI. San Francisco, CA: United Nations, October 24, 1945. <http://www.refworld.org/docid/3ae6b3930.html>, accessed 7 November 2017.

UN. Democracy. United Nations, <http://www.un.org/en/sections/issues-depth/democracy/index.html>. Accessed 21 April 2018.

UN General Assembly. Measures to be taken against propaganda and the inciters of a new war, A RES 110 (II) § (1947). <https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/038/17/IMG/NR003817.pdf?OpenElement>, accessed 7 November 2017.

UN, General Assembly. "General Assembly Adopts Resolution Calling upon States Not to Recognize Changes in Status of Crimea Region." New York, NY: United Nations General Assembly, March 27, 2014.

<http://www.un.org/press/en/2014/ga11493.doc.htm>. Accessed 19 March 2016.

UN General Assembly. International Covenant on Civil and Political Rights. United Nations, 16 Dec. 1966,

<http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

UN General Assembly. Universal Declaration of Human Rights. United Nations, 1948, <https://www.un.org/en/universal-declaration-human-rights/index.html>.

UN, Security Council. "SECURITY COUNCIL CONDEMNS NUCLEAR TEST BY DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA." Resolution 1718 (2006). United Nations, October 14, 2006. <http://www.un.org/press/en/2006/sc8853.doc.htm>. Accessed 19 March 2016.

UN, Security Council. "Security Council Condemns Democratic People's Republic of Korea Nuclear Test, Toughens Sanctions." Resolution. 1874 (2009). United Nations, June 12, 2009. <http://www.un.org/press/en/2009/sc9679.doc.htm>. Accessed 19 March 2016.

UN, Security Council. "Security Council Condemns Use of Ballistic Missile Technology in Launch by Democratic People's Republic of Korea, in Resolution 2087 (2013)." Resolution. 2087. New York, NY: United Nations Security Council, January 22, 2013. <https://www.un.org/press/en/2013/sc10891.doc.htm>. Accessed 9 January 2018.

UN, Security Council. "Security Council Imposes Fresh Sanctions on Democratic People's Republic of Korea, Unanimously Adopting Resolution 2270 (2016)." Resolution. New York, NY: United Nations Security Council, March 2, 2016. <https://www.un.org/press/en/2016/sc12267.doc.htm>. Accessed 9 January 2018.

UN, Security Council. "Security Council Toughens Sanctions Against Democratic People's Republic of Korea, Unanimously Adopting Resolution 2371 (2017)." Resolution. New York, NY: United Nations Security Council, August 5, 2017. <https://www.un.org/press/en/2017/sc12945.doc.htm>. Accessed 9 January 2018.

UN, Security Council. "UN Security Council Resolution 2166 Condemning Downing of Malaysia Airlines Flight MH17." New York, NY: United Nations Security Council, July 21, 2014. http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2166.pdf. Accessed 19 March 2016.

UN, Security Council. "Security Council Imposes Additional Sanctions on Iran, Voting 12 in Favour to 2 Against, with 1 Abstention." New York, NY: United Nations, June 9, 2010. <http://www.un.org/press/en/2010/sc9948.doc.htm>. Accessed 19 March 2016.

U.S. Army Field Manual 3-13, *Inform and Influence Activities*, Headquarters, Department of the Army, Washington, DC, January 2013.

U.S. Army Field Manual 3-36, *Electronic Warfare Techniques*, Washington, DC: Headquarters, Department of the Army, 2014.

U.S. Army Field Manual 3-38, *Cyber Electromagnetic Activities*, Headquarters, Department of the Army, Washington, DC, 12 February 2014.

U.S. Army. *Special Forces Guide to Information Operations*. TC - Training Circular 18-06. Washington, DC: Headquarters, Department of the Army, March 2013.

U.S. Department of Defense, "Joint Publication 1: Doctrine for the Armed Forces of the United States." U.S. Department of Defense, March 25, 2013. http://www.dtic.mil/doctrine/new_pubs/jp1.pdf, accessed 2 April 2, 2016.

U.S., Department of State. "Under Secretary for Public Diplomacy and Public Affairs." U.S. Department of State. Accessed July 25, 2016. <http://www.state.gov/r/>, accessed 25 July 2016.

U.S. Information Agency, archived website from the agency's closing in 1999, archive maintained by the Electronic Research Collection, historic State Department materials, federal depository library, University of Illinois at Chicago, <http://dosfan.lib.uic.edu/usia/>, accessed 21 May 2016.

U.S. Joint Publication 3-13, *Information Operations*, 20 November 2014. Joint Publication 3-13, U.S. Joint Chiefs of Staff, 27 November 2012 with Change 1 effective 20 November 2014.

U.S. Joint Staff Joint Publication 3-12 (R), *Cyberspace Operations*, 5 February 2013. Joint Publication, 3-12 (R), U.S. Joint Chiefs of Staff, 2013.

U.S. Joint Publication 3-13.2, *Military Information Support Operations*, Joint Publication 3-13.2, U.S. Joint Chiefs of Staff, 2010.

U.S. National Archives, Records of the U.S. Information Agency (RG 306), Cold War Era Agencies, <https://www.archives.gov/research/foreign-policy/related-records/rg-306.html>, accessed 21 May 2016.

Waltz, Kenneth N. "Nuclear Myths and Political Realities." *The American Political Science Review*. Vol. 84, No. 3 (Sep, 1990), pp. 731–746

Waltz, Kenneth N., *The Spread of Nuclear Weapons: A Debate Renewed*. W. W. Norton & Company. New York: 1995

Weedon, Jen, William Nuland, and Alex Stamos. "Information Operations and Facebook." *Facebook*, April 27, 2017.

Williams, Carol J. "Russia Ends Broadcasts by Voice of America 'Propaganda' Tool." *Los Angeles Times*, April 11, 2014. <http://articles.latimes.com/2014/apr/11/world/la-fg-wn-russia-voice-of-america-20140411>. Accessed 20 March 2016.

Williams, Martyn. "How Digital Technology Gets the News out of North Korea". *PCWorld*, 1 November 2010. http://www.pcworld.com/article/209383/how_digital_technology_gets_the_news_out_of_north_korea.html?tk=rss

Wilson, Woodrow: "Executive Order 2594 - Creating Committee on Public Information," April 13, 1917. Online by Gerhard Peters and John T. Woolley, *The American Presidency Project*. <http://www.presidency.ucsb.edu/ws/?pid=75409>, accessed 25 July 2016.

Whitton, John B. "Cold War Propaganda." *American Society of International Law* 45, no. 1 (January 1951): 151–53. <https://doi.org/10.2307/2194791>, accessed 6 November 2017.

Wolfsthal, Jon. "The intelligence 'black hole' over N Korea". *BBC News*, 17 July 2003. <http://news.bbc.co.uk/2/hi/asia-pacific/3073677.stm>.

Xindex, "North Korea Is Deleting History." *Xindex*, December 16, 2013.
<https://www.indexonensorship.org/2013/12/north-korea-deleting-history/>

Yonhap, "(5th LD) Two Koreas Exchange Shells over Western Border." Yonhap.
August 20, 2015, online edition.
<http://english.yonhapnews.co.kr/search1/2603000000.html?cid=AEN20150820011155315>. Accessed 12 January 2018.

Yoo Jee-ho. "North to freeze Kumgang assets from tomorrow." *JoongAng Daily* [newspaper], 12 April 2010.
<http://joongangdaily.joins.com/article/view.asp?aid=2919066>.

Yoo, Jee-ho. "Marines Recall Yeonpyeong Shelling with Anger, New Perspective." Yonhap. November 21, 2011, online edition, sec. Politics/Diplomacy.
<http://english.yonhapnews.co.kr/national/2011/11/18/12/0301000000AEN20111118002400315F.HTML>. Accessed 13 January 2018.

Yoon Won-joon. "Pak Nam-gi Executed; Live Communications with North via Satellite Phone." *Donga Ilbo* [newspaper], 22 March 2010. Translation by author.
<http://news.donga.com/Politics/New/3/00/20100322/27000532/1&top=1>.

Zakaria, Tabassum, and Arshad Mohammed. "RPT-Mission Impossible? U.S. Wants Sanctions to Hurt Only Iran." *Reuters*, February 17, 2012.
<http://www.reuters.com/article/usa-iran-sanctions-idUSL2E8DD9TD20120217>. Accessed 19 March 2016.