International Security

After Deterrence Explaining Conflict Short of War

--Manuscript Draft--

Manuscript Number:	
Full Title:	After Deterrence Explaining Conflict Short of War
Short Title:	After Deterrence
Article Type:	Article
Corresponding Author:	J Andres Gannon University of California San Diego San Diego, CA UNITED STATES
Corresponding Author Secondary Information:	
Corresponding Author's Institution:	University of California San Diego
Corresponding Author's Secondary Institution:	
First Author:	J Andres Gannon
First Author Secondary Information:	
Order of Authors:	J Andres Gannon
	Erik Gartzke, PhD
	Jon R. Lindsay, PhD
Order of Authors Secondary Information:	
Abstract:	Russia’s intervention in Ukraine highlighted an emerging phenomenon of conflict in the “gray zone” between peace and war. Is limited conflict, leveraging novel tactics and technologies, an effective way to subvert deterrence—as many believe—or does it reflect deterrence success? While limited war is nothing new, most attention has focused on conflict with weaker, irregular actors that possess limited means. Gray zone conflict, by contrast, involves stronger, nation-state actors with limited ends. There are two reasons why capable actors might choose to employ only a subset of their capabilities. Actors may limit their efforts for the sake of efficiency if their objectives require only limited means. Alternatively, voluntary limits may reflect concerns about the potential risks of escalation. Actions in the gray zone thus pose a discrimination problem: aggressors motivated by efficiency are more inclined to escalate if challenged, while aggressors concerned about deterrence should tend to back down. Indeed, if gray zone conflict is a reaction to deterrence, its scope and intensity should vary inversely with the credibility of deterrence. Drawing on Russian aggression, we find support for the deterrence hypothesis in qualitative and quantitative data. Gray zone conflict is better understood as a reflection of weakness than as an expression of strength.
Suggested Reviewers:	Michael Poznansky, PhD University of Pittsburgh poznansky@pitt.edu Knowledgeable about contemporary cyber operations
	Austin Carson, PhD University of Chicago acarson@uchicago.edu Knowledgeable about great power conflict short of war
	Daniel Maliniak, PhD William and Mary dxmali@wm.edu Knowledgeable about recent Russian incursions in eastern Europe
Opposed Reviewers:	

To whom it may concern,

Please find attached our paper, "After Deterrence: Explaining Conflict Short of War" for consideration at *International Security*. The manuscript advances a new theoretical contribution explaining the modern phenomenon of "gray zone conflict" and empirically assesses that theory using new data on Russian interventions since 1994.

The paper has previously been presented at the 2016 ISAC-ISSS Conference, 2018 STRATCOM Deterrence Symposium, and the 2018 American Political Science Association Conference. Colleagues who have given us feedback on earlier versions and would thus likely not be double-blind peer reviewers include Peter Schram, Nadiya Kostyuk, Chris Whyte, and Chad Levinson. Co-panelists at these conferences include Lindsey O'Rourke, Monica Lee, Will Nuland, and Ahmed Zohny. We suggest reviewers who are knowledgeable about the theoretical approach of the deterrence and spiral models of conflict and/or conflict short of war as well as reviewers who can assess our empirical claims about Russian intervention in the 21st century.

This research was sponsored by Office of Naval Research Grant N00014-14-1-0071 and the Department of Defense Minerva Research Initiative. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the view of the U.S. government.

Thank you,

J Andres Gannon, Erik Gartzke, and Jon R. Lindsay

After Deterrence:
Explaining Conflict Short of War[1]

J Andres Gannon[1], Erik Gartzke[2], and Jon R. Lindsay[3]

[1]*Department of Political Science , University of California, San Diego*
[2]*Director, Center for Peace and Security Studies (cPASS), Department of Political Science, University of California, San Diego*
[3]*Munk School of Global Affairs & Public Policy, Department of Political Science, University of Toronto*

June 2019

Abstract: Russia's intervention in Ukraine highlighted an emerging phenomenon of conflict in the "gray zone" between peace and war. Is limited conflict, leveraging novel tactics and technologies, an effective way to subvert deterrence—as many believe—or does it reflect deterrence success? While limited war is nothing new, most attention has focused on conflict with weaker, irregular actors that possess limited means. Gray zone conflict, by contrast, involves stronger, nation-state actors with limited ends. There are two reasons why capable actors might choose to employ only a subset of their capabilities. Actors may limit their efforts for the sake of efficiency if their objectives require only limited means. Alternatively, voluntary limits may reflect concerns about the potential risks of escalation. Actions in the gray zone thus pose a discrimination problem: aggressors motivated by efficiency are more inclined to escalate if challenged, while aggressors concerned about deterrence should tend to back down. Indeed, if gray zone conflict is a reaction to deterrence, its scope and intensity should vary inversely with the credibility of deterrence. Drawing on Russian aggression, we find support for the deterrence hypothesis in qualitative and quantitative data. Gray zone conflict is better understood as a reflection of weakness than as an expression of strength.

Abstract: 205 words

Article: 14,944 words (excluding title page, including footnotes)

J Andres Gannon, Erik Gartzke, and Jon R. Lindsay

[1] The authors wish to thank the members of the Center for Peace and Security Studies (cPASS), particularly Rex Douglass, Tom Scherer, and Peter Schram, as well as Nadiya Kostyuk, Chad Levinson, and John Warden for thoughtful feedback. Tom Brailey, Cole Reynolds, Benjamin Smalley, and Erin Werner provided excellent research assistance. Earlier drafts of this paper were presented at the 10th Annual Strategic Multi-layer Assessment (SMA) Conference, the 2016 ISAC-ISSS Annual Conference, the Digital Issues Discussion Group (DIDG), the 2018 STRATCOM Deterrence Symposium, and the 2018 American Political Science Association conference, Boston, MA. This research was sponsored by Office of Naval Research Grant N00014-14-1-0071 and the Department of Defense Minerva Research Initiative. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the view of the U.S. government.

After Deterrence: Explaining Conflict Short of War

June 2019

Russia's intervention in Ukraine highlighted an emerging phenomenon of conflict in the "gray zone" between peace and war. Is limited conflict, leveraging novel tactics and technologies, an effective way to subvert deterrence—as many believe—or does it reflect deterrence success? While limited war is nothing new, most attention has focused on conflict with weaker, irregular actors that possess limited means. Gray zone conflict, by contrast, involves stronger, nation-state actors with limited ends. There are two reasons why capable actors might choose to employ only a subset of their capabilities. Actors may limit their efforts for the sake of efficiency if their objectives require only limited means. Alternatively, voluntary limits may reflect concerns about the potential risks of escalation. Actions in the gray zone thus pose a discrimination problem: aggressors motivated by efficiency are more inclined to escalate if challenged, while aggressors concerned about deterrence should tend to back down. Indeed, if gray zone conflict is a reaction to deterrence, its scope and intensity should vary inversely with the credibility of deterrence. Drawing on Russian aggression, we find support for the deterrence hypothesis in qualitative and quantitative data. Gray zone conflict is better understood as a reflection of weakness than as an expression of strength.

Word Count: 15166 (including title page and abstract)

Introduction

In the wake of the overthrow of Ukrainian President Viktor Yanukovych in February 2014, the Crimean Peninsula was invaded by "little green men," soldiers whose uniforms lacked insignia or other identifying information. While nobody seriously doubted the origin of these troops, the pretext of anonymity afforded NATO a fig leaf—had they needed one—to avert direct confrontation between West and East.[1] The Kremlin formally annexed Crimea shortly thereafter. Russian intervention in Ukraine continues to this day, consisting of limited ground operations and aggressive cyber campaigns.[2] Many now worry about a potential repeat performance in the Baltics, where ethnic Russian minorities and NATO membership make for a dangerous mix. Other Russian "active measures" similarly appear to be designed to undermine the legitimacy of Western democratic institutions and to inflame the wave of nationalist populism opposed to the "liberal international order," while ensuring that military confrontation between Russia and NATO does not take place.[3]

According to the former British Defense Secretary, Michael Fallon, "That is not a Cold War. It is a grey war. Permanently teetering on the edge of outright hostility. Persistently hovering around the threshold of what we would normally consider acts of war".[4] The imagery of little green men in "the gray zone" has even been extended to "little blue men" used by China to erode "red lines" in maritime East Asia.[5] The kaleidoscopic language highlights both practical

[1] NATO is not formally bound to assist Ukraine, but neither are they precluded from doing so. The issue for the Kremlin was ensuring that Brussels remained passive, and any measure that might help was worth taking.

[2] Michael Kofman et al., "Lessons from Russia's Operations in Crimea and Eastern Ukraine," Product Page (Santa Monica, CA: Rand Corporation, 2017), https://www.rand.org/pubs/research_reports/RR1498.html; A. F. Brantly, N. Cal, and D. Winkelstein, "Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW," Report (Army Cyber Institute, December 1, 2017), https://vtechworks.lib.vt.edu/handle/10919/81979; Robert Angevine et al., "Learning Lessons from the Ukraine Conflict" (Institute for Defense Analyses, May 2019).

[3] Christopher Paul and Miriam Matthews, "The Russian ``Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It" (Santa Monica, CA: Rand Corporation, 2016); Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *The New York Times*, October 12, 2016, sec. World, https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html; Seth G Jones, "Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare," Brief (Washington, D.C: Center for Strategic and International Studies, October 2018).

[4] Michael Fallon, "Speech Delivered by Secretary of State for Defence Sir Michael Fallon at the RUSI Landwarfare Conference.," (Speech, June 28, 2017), https://www.gov.uk/government/speeches/rusi-landwarfare-conference.

[5] Andrew S. Erickson and Connor Kennedy, "Directing China's 'Little Blue Men': Uncovering the Maritime Militia Command Structure," CSIS Asia Maritime Transparency Initiative, September 11, 2015, https://amti.csis.org/directing-chinas-little-blue-men-uncovering-the-maritime-militia-command-structure/; Michael Green et al., *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (Rowman & Littlefield, 2017); Van Jackson, "Tactics of Strategic Competition: Gray Zones, Redlines, and Conflict before War," *Naval War College Review* 70, no. 3 (2017): 39–61; Erik Lin-Greenberg, "Non-Traditional Security Dilemmas: Can Military Operations Other than War Intensify Security Competition in Asia?," *Asian Security* 0, no. 0 (December 27, 2017): 1–21, https://doi.org/10.1080/14799855.2017.1414044.

and conceptual challenges in the practice of deterrence. As the Chairman of the Joint Chiefs of Staff noted, “Our traditional approach is either we’re at peace or at conflict. And I think that’s insufficient to deal with the actors that actually seek to advance their interests while avoiding our strengths”.[6]

These concerns reflect widely held, yet problematic, beliefs that gray zone conflict is either a thoroughly novel, or especially potent, form of warfare. Limited war is an old problem, even as most attention has focused on irregular actors limited by means rather than capable actors pursuing limited ends. Russia and other countries appear to be outsmarting the West by utilizing new technologies, or combinations of capabilities in different domains, to undermine traditional defenses and revise the balance of power. Challengers seem to be undeterred from using cyber-enabled aggression as an efficient way to pursue their interests. We argue, by contrast, that gray zone conflict is a symptom of Western success. The explicit declaratory statements and implicit relative power of the stronger coalition limit maneuver room for the weaker revisionist. Covert intervention and cyber campaigns are better understood as sub-optimal, “second-best” strategies for maximizing political-military influence, which would be more effectively achieved through overt intervention, although at increased cost and risk. In sum, gray zone actors do not care enough to send the very best.

The good news in our version of events is that gray zone conflict is a response to deterrence success. The severity of gray zone conflict should then be attenuated wherever the defender’s power and resolve are higher. The bad news in this conception is that gray zone conflict probes the threshold of deterrence effectiveness. Thus, conflict severity should be greater where defender power and resolve is more questionable. A nation’s interests will vary across different issue areas, as will its ability to project military power to back up deterrent threats. Therefore, we expect the intensity and lethality of conflict to vary along a gradient of deterrence credibility, analogous to the military loss of strength gradient across geographical distance.[7] We test this hypothesis by drawing on a new dataset of Russian interventions since the end of the Cold War and qualitative studies of Russia’s major cyber campaigns, which vary in the additional types of force that Russia has mobilized. We find that Russia systematically limits its choice of military means along an East-West gradient, behaving more furtively as Western credibility increases.

Deterrence shapes the way that conflict emerges, but it cannot suppress conflict altogether. An adversary is seldom passive. There will always be attempts at end-runs or push-back, even when deterrence is credible. It is also important to avoid overextending commitments where credibility is in doubt. Policymakers should be sensitive to the deterrence gradient,

[6] Joseph Dunford, “Gen. Dunford’s Remarks and Q&A at the Center for Strategic and International Studies” (Remarks, March 29, 2016), http://www.jcs.mil/Media/Speeches/Article/707418/gen-dunfords-remarks-and-qa-at-the-center-for-strategic-and-international-studi/.

[7] Kenneth E Boulding, *Conflict and Defense: A General Theory* (New York: Harper, 1962).

seeking to reinforce success and respect weakness. We make our argument in four parts. First, we locate gray zone conflict in the broader literature on limited war. Second, we analyze limited conflict through the lens of deterrence theory. Third we conduct a plausibility probe of our argument using recent Russian cases. We conclude with implications of our argument.

Between Peace and War

There is nothing new about conflict that falls ambiguously between peace and war.[8] There is a long history of, and a vast literature on, limited conflict, salami tactics, low intensity conflict, revolutionary war, military operations other than war, covert operations, small wars, and proxy wars.[9] Many (but not all) of these concepts emphasize asymmetric struggles with

[8] Mark Galeotti, "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?," *Small Wars & Insurgencies* 27, no. 2 (March 3, 2016): 282–301, https://doi.org/10.1080/09592318.2015.1129170.

[9] On limited conflict, see Henry A. Kissinger, "Military Policy and Defense of the 'Grey Areas,'" *Foreign Affairs* 33, no. 3 (1955): 416–28, https://doi.org/10.2307/20031108; Thomas C. Schelling, "Bargaining, Communication, and Limited War," *Conflict Resolution* 1, no. 1 (1957): 19–36; Robert E. Osgood, "The Reappraisal of Limited War," *The Adelphi Papers* 9, no. 54 (February 1969): 41–54, https://doi.org/10.1080/05679326908448127; Stephen Peter Rosen, "Vietnam and the American Theory of Limited War," *International Security* 7, no. 2 (1982): 83–113, https://doi.org/10.2307/2538434; Joseph Lepgold and Brent L. Sterling, "When Do States Fight Limited Wars?: Political Risk, Policy Risk, and Policy Choice," *Security Studies* 9, no. 4 (June 1, 2000): 127–66, https://doi.org/10.1080/09636410008429415; Patricia L. Sullivan, "War Aims and War Outcomes Why Powerful States Lose Limited Wars," *Journal of Conflict Resolution* 51, no. 3 (June 1, 2007): 496–524, https://doi.org/10.1177/0022002707300187; Robert Powell, "Nuclear Brinkmanship, Limited War, and Military Power," *International Organization* 69, no. 03 (June 2015): 589–626, https://doi.org/10.1017/S0020818315000028. On salami tactics, see Thomas C. Schelling, *Arms and Influence* (Yale University Press, 1966); James Fearon, "Bargaining Over Objects That Influence Future Bargaining Power" (Draft, October 1996); Lawrence Freedman, "Ukraine and the Art of Limited War," *Survival* 56, no. 6 (November 2, 2014): 7–38, https://doi.org/10.1080/00396338.2014.985432; Steven Metz, "Foundation for a Low Intensity Conflict Strategy," *Comparative Strategy* 8, no. 2 (January 1989): 265–73, https://doi.org/10.1080/01495938908402780. On low intensity conflict, see Robert C. Freysinger, "US Military and Economic Intervention in an International Context of Low-Intensity Conflict," *Political Studies* 39, no. 2 (June 1, 1991): 321–34, https://doi.org/10.1111/j.1467-9248.1991.tb01370.x; Arthur V. Grant, "Strategic Decisions: The Mire of Low-Intensity Conflict," *Comparative Strategy* 10, no. 2 (April 1, 1991): 165–75, https://doi.org/10.1080/01495939108402840; Graham H Turbiville, "Preface: Future Trends in Low Intensity Conflict," *Low Intensity Conflict & Law Enforcement* 11, no. 2–3 (June 1, 2002): 155–63, https://doi.org/10.1080/0966284042000279957. On revolutionary war, see John Shy and Thomas W. Collier, "Revolutionary War," in *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, ed. Peter Paret, Gordon A Craig, and Felix Gilbert (New Jersey: Princeton University Press, 1986), 815–62. On military operations other than war, see Stuart Kinross, "Clausewitz and Low-Intensity Conflict," *Journal of Strategic Studies* 27, no. 1 (March 1, 2004): 35–58, https://doi.org/10.1080/0140239042000232765; Lin-Greenberg, "Non-Traditional Security Dilemmas". On covert operations, see Loch K. Johnson, "On Drawing a Bright Line for Covert Operations," *The American Journal of International Law* 86, no. 2 (1992): 284–309, https://doi.org/10.2307/2203235; Austin Carson, *Secret Wars: Covert Conflict in International Politics*, Princeton Studies in International History and Politics (Princeton, NJ: Princeton University Press, 2018); Lindsey A. O'Rourke, *Covert Regime Change: America's Secret Cold War*, Cornell Studies in Security Affairs (Ithaca, NY: Cornell University Press, 2018). On small wars, see William Olson, "The Concept of Small Wars," *Small Wars & Insurgencies* 1, no. 1 (April 1, 1990): 39–46, https://doi.org/10.1080/09592319008422940. On proxy wars, see Yaacov Bar-Siman-Tov, "The Strategy of War by Proxy," *Cooperation and Conflict* 19, no. 4 (1984): 263–273; Seyom Brown, "Purposes and Pitfalls of War by Proxy: A Systemic Analysis," *Small Wars &*

combatants that are *unable* in material terms to fight on a larger scale or with higher intensity.

The interesting puzzle about gray zone conflict, as we will use the term here, is that adversaries are *unwilling* to broaden the scope or intensity of a military engagement, despite being able to do so. But this also is not a new phenomenon. In 1978 Henry Kissinger advocated for "an intelligence community that, in certain complicated situations, can defend the American national interest in the gray areas where military operations are not suitable and diplomacy cannot operate".[10] General Joseph Votel has described the Cold War as "a 45-year-long Gray Zone struggle" in which the United States and Soviet Union conducted proxy wars, covert operations, and (dis)information campaigns against one another while avoiding a direct military and likely nuclear confrontation. Cold War deterrence shaped the modality and severity of conflict that occurred, but it did not, and could not, eliminate it completely[11]. Today many are concerned about an emerging manifestation of limited war, often called "gray zone conflict." United States Special Operations Command (SOCOM) has defined it as:

> a conceptual space between peace and war occurring when actors purposefully use single or multiple elements of power to achieve political-security objectives with activities that are typically ambiguous or cloud attribution and exceed the threshold of ordinary competition, yet intentionally fall below the level of large-scale direct military conflict and threaten US and allied interests by challenging, undermining, or violating international customs, norms, or laws.[12]

Again, this is not a new problem. While it is convenient to think of peace and war as dichotomous, discrete outcomes, observers have long recognized that tension and violence exist on a spectrum, even as the language used to describe it evolves.[13] The Cold War featured three distinct threads of thought dealing with limited war: aggressive peacetime competition and intelligence operations vis-a-vis the Soviet Union (war limited by ends), conventional

Insurgencies 27, no. 2 (March 3, 2016): 243–57, https://doi.org/10.1080/09592318.2015.1134047; Jesse Driscoll and Daniel Maliniak, "With Friends Like These: Brinkmanship and Chain-Ganging in Russia's Near Abroad," *Security Studies* 25, no. 4 (October 1, 2016): 585–607, https://doi.org/10.1080/09636412.2016.1220208.

[10] Loch K. Johnson, "The Myths of America's Shadow War," *The Atlantic*, January 31, 2013, https://www.theatlantic.com/international/archive/2013/01/the-myths-of-americas-shadow-war/272712/.

[11] Joseph Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly* 80 (January 2016), http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf.

[12] Belinda Bragg, "Integration Report: Gray Zone Conflicts, Challenges, and Opportunities," Strategic Multi-Layer Assessment (SMA) (Arlington, VA, July 2017), http://nsiteam.com/social/wp-content/uploads/2017/07/Integration-Report-Final-07-13-2017-R.pdf.

[13] Richard Ned Lebow, "The Past and Future of War," *International Relations* 24, no. 3 (September 1, 2010): 243–70, https://doi.org/10.1177/0047117810377277.

war in the shadow of nuclear weapons (war limited by risks), and low-intensity conflict with irregular forces (war limited by means).

Wars Limited by Ends

In the early days of the Cold War, George Kennan emphasized that both overt and covert political warfare could play a role in long-term strategic competition with the Soviet Union.

> Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures..., and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states.[14]

The emphasis on limited political objectives over military operations represented an important shift in thinking. The Korean War exemplified an underappreciated type of war fought to achieve political ends short of traditional military victory despite having the capability to do so.[15] Contemporary treatment understood limited war as a conflict between actors who had the capacity to increase battlefield commitment but did not want to do so, creating a third option short of major war yet beyond acquiescence.[16] Kissinger and Osgood tried to figure out ways to conduct limited war and avoid escalation by restricting targets and weapons systems or limiting the geographic scope of conflict.[17] This form of war, ironically, and challengingly, required some tacit agreement or common conjecture among adversaries to limit the scope of war.[18] During the Vietnam war, for instance, the North Vietnamese leadership was prepared to escalate conflict even as China and the Soviet Union worked to restrain their ally.[19]

[14] George Kennan, "269. Policy Planning Staff Memorandum," Records of the National Security Council NSC 10/2 (Washington: National Archives and Records Administration, May 4, 1948), http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm.

[15] Osgood, "The Reappraisal of Limited War"; R. Harrison Wagner, "Bargaining and War," *American Journal of Political Science* 44, no. 3 (2000): 469–84, https://doi.org/10.2307/2669259.

[16] Kissinger, "Military Policy and Defense of the 'Grey Areas'"; Bernard Brodie, "More About Limited War," ed. RN Rear Admiral Sir Anthony W. Buzzard, Robert E. Osgood, and P. M. S. Blackett, *World Politics* 10, no. 1 (1957): 112–22, https://doi.org/10.2307/2009228; Henry A. Kissinger, "Strategy and Organization," *Foreign Affairs* 35, no. 3 (1957): 379–94, https://doi.org/10.2307/20031235.

[17] Dr Stewart Woodman, "Defining Limited Conflict: A Case of Mistaken Identity," *Small Wars & Insurgencies* 2, no. 3 (December 1, 1991): 24–43, https://doi.org/10.1080/09592319108422992.

[18] Schelling, "Bargaining, Communication, and Limited War."

[19] Michael Carver, "Conventional Warfare in the Nuclear Age," in *Makers of Modern Strategy from Machiavelli to the Nuclear Age.*, ed. Peter Paret, Gordon A Craig, and Felix Gilbert (New Jersey: Princeton University Press, 1986), 779–814, http://public.eblib.com/choice/publicfullrecord.aspx?p=827816.

Wars Limited by Risk

Cold War strategists advanced the notion of "the stability-instability paradox" to explain how incentives for engaging in conflict at lower levels of intensity or in peripheral theaters arise out of disincentives for initiating nuclear war (or even major conventional war).[20] According to Snyder, "nuclear technology introduced a new form of intent-perception and a new form of uncertainty — that concerning what types of military capability the opponent was likely to use and what degree of violence he was willing to risk or accept."[21] The presence of nuclear weapons might prevent world war, but it could simultaneously encourage localized aggression or smaller, more limited conflicts.[22] At the same time, the feasibility of "weakening the enemy with pricks instead of blows" is limited by the implicit risk of nuclear escalation.[23] Modern studies evaluate stability-instability quantitatively or in specific regions.[24]

Recent formalizations of limited conflict in the shadow of major war point to the need for updated conceptions of deterrence. Schelling argued that "the main consequence of limited war, and potentially a main purpose for engaging in it, is to raise the risk of larger war."[25] Gray zone conflict poses a different relationship in which a capable actor may choose to engage in limited war precisely to *lower* the risk of larger war.[26] As Powell states, "the amount of power the challenger brings to bear affects the stability of the conflict. More specifically, how much power the challenger brings to bear limits how much risk the

[20] Glenn Snyder, "The Balance of Power and the Balance of Terror," in *World in Crisis: Readings in International Relations*, ed. Frederick Hartmann (New York: The Macmillan Company, 1965), 180–91; Robert Jervis, *The Illogic of American Nuclear Strategy* (Cornell University Press, 1984).

[21] Snyder, "The Balance of Power and the Balance of Terror."

[22] Richard L. Russell, "The Nuclear Peace Fallacy: How Deterrence Can Fail," *Journal of Strategic Studies* 26, no. 1 (March 1, 2003): 136–55, https://doi.org/10.1080/01402390308559311; Scott Douglas Sagan and Kenneth Neal Waltz, *The Spread of Nuclear Weapons: A Debate Renewed* (Norton, 2003); S. Paul Kapur, *Dangerous Deterrent: Nuclear Weapons Proliferation and Conflict in South Asia* (Stanford University Press, 2007).

[23] Sir Basil Henry Liddell Hart, *Strategy: The Indirect Approach* (Faber & Faber, 1954).

[24] R. Rauchhaus, "Evaluating the Nuclear Peace Hypothesis: A Quantitative Approach," *Journal of Conflict Resolution* 53, no. 2 (January 27, 2009): 258–77, https://doi.org/10.1177/0022002708330387; Bryan Early and Victor Asal, "Nuclear Weapons, Existential Threats, and the Stability–Instability Paradox," *The Nonproliferation Review* 0, no. 0 (October 2, 2018): 1–25, https://doi.org/10.1080/10736700.2018.1518757; Sumit Ganguly, "Indo-Pakistani Nuclear Issues and the Stability/Instability Paradox," *Studies in Conflict & Terrorism* 18, no. 4 (January 1, 1995): 325–34, https://doi.org/10.1080/10576109508435989; V.R. Raghavan, "Limited War and Nuclear Escalation in South Asia," *The Nonproliferation Review* 8, no. 3 (September 2001): 82–98, https://doi.org/10.1080/10736700108436865; Terence Roehrig, "North Korea, Nuclear Weapons, and the Stability-Instability Paradox," *Korean Journal of Defense Analysis* 28, no. 2 (June 2016): 181–98.

[25] Schelling, *Arms and Influence*.

[26] Peter Schram, "Better Living Through Hassling: How to Prevent a Preventative War" (Working Paper, 2019).

defender can generate".[27] Mutually constrained actors pursue (and resist) aggression furtively, so as to protect broader cooperative or compatible goals.

Deterrence is really a strategy designed to buy time against an adversary committed to changing the status quo. George and Smoke raise the issue of "designing around" deterrence as adversaries seek out options that "offers an opportunity for gain while minimizing the risk of an unwanted response by the defender".[28] Sometimes this can result in serious fighting as when Egypt "designed around" Israel's deterrent in 1973.[29] Even so, "designing around" deterrence remains a perverse symptom of its success if the adversary limits its means and aims, even in cases where the target panics or fears that the attacker's aims are not limited (as Israel did). Others share this perspective. Lieberman argues that "designing around" is a sign of deterrence success if an adversary shapes its challenge in response to the anticipated reaction of the defender.[30]

Wars Limited by Means

The Cold War witnessed numerous decolonization struggles and proxy wars in the Third World. Limited war with irregular forces rather than a peer competitor directly garnered much attention in the 1970s under the rubric of "low intensity conflict" or LIC.[31] Some treatments of LIC focus on the use of light weapons and ambush tactics while others identify the phenomenon in terms of non-state actors.[32] The common focus is on strategies of the weak. Unsurprisingly LIC is more prevalent in under-developed or poorly institutionalized

[27] Powell, "Nuclear Brinkmanship, Limited War, and Military Power."

[28] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (Columbia University Press, 1974); Alexander L. George and Richard Smoke, "Deterrence and Foreign Policy," *World Politics* 41, no. 2 (1989): 170–82, https://doi.org/10.2307/2010406.

[29] Janice Gross Stein, "Calculation, Miscalculation, and Conventional Deterrence," in *Psychology and Deterrence*, by Richard Ned Lebow and Robert Jervis (JHU Press, 1989).

[30] Elli Lieberman, *Reconceptualizing Deterrence: Nudging Toward Rationality in Middle Eastern Rivalries* (Routledge, 2012).

[31] George Schultz, "Low-Intensity Warfare: The Challenge of Ambiguity" (Conference Address, January 15, 1986), https://www.jstor.org/stable/pdf/20692938.pdf.

[32] Analysis of tactics can be found in Peter Kornbluh and Joy Hackel, "Low-Intensity Conflict Is It Live or Is It Memorex?," *NACLA Report on the Americas* 20, no. 3 (June 1986): 8–11, https://doi.org/10.1080/10714839.1986.11723411; Thomas K. Adams, "LIC (Low Intensity Clausewitz)," *Small Wars and Insurgencies* 1, no. 3 (December 1, 1990): 266–75, https://doi.org/10.1080/09592319008422959. A focus on non-state actors is provided in Richard D. Downie, "Low Intensity Conflict Doctrine and Policy: Old Wine in a New Bottle?," *Studies in Conflict & Terrorism* 15, no. 1 (January 1, 1992): 53–67, https://doi.org/10.1080/10576109208435891; Kinross, "Clausewitz and Low-Intensity Conflict."

regions.[33] The classical literature on counterinsurgency and its modern variants fall into this category.[34]

Wars with means-limited actors have received most of the attention after the Cold War as the United States has been involved in a long series of peacekeeping operations and grueling counterinsurgencies. A vast academic literature on civil war has emerged in recent years to explain the behavior, motives and organizational structure of irregular actors and the militaries that fight them.[35] The recent renewal of interest in low-intensity conflict between more capable competitors in many ways represents a return to the two earlier themes—wars limited by ends and risk-sensitivity.

Modern Gray Zone Conflict

Gray zone conflict today has been described as "a carefully planned campaign operating in the space between traditional diplomacy and overt military aggression" employed by revisionist states with grand geopolitical ambitions and irresistible capabilities.[36] This pessimism has even led some to advocate revamping deterrence to focus on threats from the gray zone.[37] Russia, and its intervention in Ukraine in particular, is the paradigmatic

[33] Kornbluh and Hackel, "Low-Intensity Conflict Is It Live or Is It Memorex?"; Grant T. Hammond, "Low Intensity Conflict: War by Another Name," *Small Wars & Insurgencies* 1, no. 3 (December 1, 1990): 226–38, https://doi.org/10.1080/09592319008422957; Avi Kober, "Low-Intensity Conflicts: Why the Gap Between Theory and Practise?," *Defense & Security Analysis* 18, no. 1 (March 1, 2002): 15–38, https://doi.org/10.1080/07430170120113712.

[34] For foundational work, see David Galula, *Counterinsurgency Warfare: Theory and Practice* (Hailer Publishing, 1964); Robert Taber, *War of the Flea: The Classic Study of Guerrilla Warfare* (L. Stewart, 1965); Sir Robert Grainger Ker Thompson, *Defeating Communist Insurgency: The Lessons of Malaya and Vietnam* (F. A. Praeger, 1966); Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, Peace-Keeping* (Faber & Faber, 1971); Douglas S. Blaufarb, *The Counterinsurgency Era: U.S. Doctrine and Performance, 1950 to the Present* (Free Press, 1977). Modern iterations include John A. Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (University of Chicago Press, 2005); US Army, "Army Field Manual 3-24: Counterinsurgency," November 30, 2006, https://www.hsdl.org/?abstract&did=; David Kilcullen, *Counterinsurgency* (Hurst, 2010).

[35] On organizational structures, see Roger D. Petersen, *Resistance and Rebellion: Lessons From Eastern Europe* (Cambridge: Cambridge University Press, 2001), https://doi.org/10.1017/CBO9780511612725; Elisabeth Jean Wood, *Insurgent Collective Action and Civil War in El Salvador* (Cambridge University Press, 2003); Stathis Kalyvas, "Review of The New U.S. Army/Marine Corps Counterinsurgency Field Manual," *Perspectives on Politics* 6, no. 02 (June 2008), https://doi.org/10.1017/S1537592708081164; Paul Staniland, *Networks of Rebellion: Explaining Insurgent Cohesion and Collapse* (Cornell University Press, 2014). On the actors involved, see David H. Ucko, *The New Counterinsurgency Era: Transforming the U.S. Military for Modern Wars* (Georgetown University Press, 2009); Austin Long, *The Soul of Armies: Counterinsurgency Doctrine and Military Culture in the US and UK* (Cornell University Press, 2016); Jacqueline L. Hazelton, "The 'Hearts and Minds' Fallacy: Violence, Coercion, and Success in Counterinsurgency Warfare," *International Security* 42, no. 1 (July 1, 2017): 80–113, https://doi.org/10.1162/ISEC_a_00283.

[36] Michael Mazarr, "Mastering the Gray Zone: Understanding a Changing Era of Conflict" (Monogram, February 2, 2015), http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1303.

[37] Joshua Foust, "Can Fancy Bear Be Stopped? The Clear and Present Danger of Russian Info Ops," War on the Rocks, September 29, 2016, http://warontherocks.com/2016/09/can-fancy-bear-be-stopped-the-clear-and-present-danger-of-russian-info-ops/; Van Jackson, "Preventing Nuclear War with North Korea,"

exemplar.[38] Russia uses novel forms of "hybrid warfare" and cyber operations to facilitate increased aggression against NATO and the West.[39] This view holds that aggressors can work around adversaries' red lines to achieve coercive bargaining success without triggering escalation.[40] If so, we might expect to see Russia engaging in gray zone conflict in as many situations as possible; there is little reason to avoid undertaking an efficient form of warfare that provides significant gains at low cost. Yet, as we show, Russia regularly pulls its punches.

The familiar logic of the stability-instability paradox plays out today with different, usually lower, thresholds. Deterrence now results as much from the risk of escalation to major conventional war, or even economic disruption, as from the threat of nuclear conflagration. One potential novelty, however, exists in the growing diversity of ways (means) available through which low intensity conflict can be practiced. The emergence of new, cheaper implements of coercion, largely but not exclusively as a result of the information revolution, have made it easier than before to fight circumspect contests.[41]

Even those who are skeptical of the potency of new information technologies still tend to highlight the expanded repertoire of military strategies available for low intensity conflict, especially emphasizing online subversion, espionage, and cyber disruption.[42] Compared to historical instances of subversion this is certainly true. Yet there are also more, and more technologically sophisticated, means available for all types of warfare, to include anti-satellite weapons, hypersonic munitions, and anti-ship ballistic missiles that are only likely

Foreign Affairs, September 11, 2016, https://www.foreignaffairs.com/articles/north-korea/2016-09-11/preventing-nuclear-war-north-korea; David Santoro and Brad Blosserman, "Healey's Wrong: It's Deterrence, Stupid," War on the Rocks, October 14, 2016, http://warontherocks.com/2016/10/healeys-wrong-its-deterrence-stupid/.

[38] Kimberly Marten, "Putin's Choices: Explaining Russian Foreign Policy and Intervention in Ukraine," *The Washington Quarterly* 38, no. 2 (April 3, 2015): 189–204, https://doi.org/10.1080/0163660X.2015.1064717; Timothy Thomas, "Russia's Military Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led," *The Journal of Slavic Military Studies* 28, no. 3 (July 3, 2015): 445–61, https://doi.org/10.1080/13518046.2015.1061819.

[39] Samuel Charap, "The Ghost of Hybrid War," *Survival* 57, no. 6 (November 2, 2015): 51–58, https://doi.org/10.1080/00396338.2015.1116147; Christopher S. Chivvis, "Hybrid War: Russian Contemporary Political Warfare," *Bulletin of the Atomic Scientists* 73, no. 5 (September 3, 2017): 316–21, https://doi.org/10.1080/00963402.2017.1362903.

[40] Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," *International Affairs* 92, no. 1 (January 2016): 175–95, https://doi.org/10.1111/1468-2346.12509; Dan Altman, "Advancing without Attacking: The Strategic Game around the Use of Force," *Security Studies*, August 16, 2017, 1–31, https://doi.org/10.1080/09636412.2017.1360074; Jackson, "Tactics of Strategic Competition: Gray Zones, Redlines, and Conflict before War."

[41] Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in *Coercion: The Power to Hurt in International Politics*, ed. Kelly M. Greenhill and Peter Krause (New York, NY: Oxford University Press, 2018).

[42] Thomas Rid, "Cyberwar and Peace," 2013, https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace; Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist," *Journal of Strategic Studies* 0, no. 0 (January 10, 2019): 1–23, https://doi.org/10.1080/01402390.2018.1559152.

to be used in major war. The apparent expansion of the number and type of means observed in many conflicts in fact reflects a reduction of the range of possible means that belligerents might employ for deterrence and war. It is important not to conflate the increasing variety of tools available for conflicts of all types with the use of a subset in limited conflict. Cyber operations may be prevalent in the gray zone, but they will be prevalent in every war of the 21st century.

The silver lining to gray zone conflict is, and always has been, that it could be worse. The bad news about persistent conflict is good news about restraint. In the last decade of the Cold War, Secretary of State George Schultz expressed a note of cautious optimism in this regard:

> The ironic fact is, these new and elusive challenges have proliferated, in part, because of our success in deterring nuclear and conventional war. Our adversaries know they cannot prevail against us in either type of war. So they have done the logical thing: they have turned to other methods. Low-intensity warfare is their answer to our conventional and nuclear strength a flanking maneuver, in military terms. They hope that the legal and moral complexities of these kinds of challenges will ensnare us in our own scruples and exploit our humane inhibitions against applying force to defend our interests.[43]

A Theory of Gray Zone Conflict

Gray zone conflict occurs when militarily capable conflict initiators intentionally limit the intensity and capacity with which they conduct military or intelligence operations and the target either does not or cannot escalate the contest. Our definition reflects the conceptual and empirical reality of an overlap with other concepts, such as low intensity conflict and small wars, while at the same time emphasizing three unique attributes of conflict in the gray zone.

First, gray zone conflict results from agency rather than necessity. It is *limitation by choice*. If limited war were distinguished only by limited ends, why wouldn't actors use the most effective means for the job? Gray zone conflict further involves "pulling punches" or refraining from using one's most potent military capabilities.

Second, gray zone conflict involves *capable initiators*. In order to choose to limit means, an actor must have a portfolio of means to choose from. This differentiates the activities of Russian or American special operations forces from insurgents, even in cases where their actual operations appear similar. Even weaker states and powerful rebel groups may vary considerably in their war aims and thus may refrain from maximum effort.[44]

[43] Schultz, "Low-Intensity Warfare: The Challenge of Ambiguity."

[44] Paul Staniland, "States, Insurgents, and Wartime Political Orders," *Perspectives on Politics* 10, no. 2 (2012): 243–64.

Third, gray zone conflict must be preferred *by both sides* in a contest. Capable belligerents have the capability to escalate but they choose not to. Although consistent with the assumptions behind theories of wars limited by risk (i.e., stability-instability paradox), this theory is based on dyadic preferences, not monadic ones. The target would rather have the opponent engage in gray zone conflict than engage in overt warfare as a result of the target's reaction to the provocation. Anticipating this, the attacker selects technologies that deliberately obfuscate its intentions or complicates attribution. This is done for the benefit of the target, to relieve it from an obligation to respond forcefully to provocation, rather than for the benefit of the initiator, to enable it to escape retaliation. Tacit collusion between adversaries enables them to avoid mutually harmful escalation.[45]

A Typology of Limited Conflict

Table 1: A Typology of Limited Conflict

		Ends	
		Concessions	Conquest
Means	Smaller and less diverse forces	Small Wars	Revolutionary Wars
	Larger and more diverse forces	Gray Zone Conflicts	Major Combat Operations

Table 1 provides a typology of limited war that distinguishes means and ends. Less capable actors are limited in both the quality and quantity of force they can bring to bear. Insurgents or criminal networks may engage in small wars to extract a few concessions from the government, such as control over a particular region or smuggling routes. If they aspire to overthrow the government, however, they may embrace Maoist or jihadist strategies in pursuit of political or ideological revolution. Our first two points above (voluntary limitation by capable actors) exclude these two categories of limited war. Our third point further distinguishes types of limited war that involve actors with more and better military forces.

Powerful actors that are highly resolved to revise the status quo will tend to use as much force as they need to get the job done. A unilateral preference for conquest makes major combat operations attractive, where force is limited simply as a function of the local balance of power. More resistance can always be met with more force, but overkill wastes resources

[45] Austin Carson, "Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War," *International Organization* FirstView (October 2015): 1–29, https://doi.org/10.1017/S0020818315000284; Carson, *Secret Wars: Covert Conflict in International Politics*.

unnecessarily. If capable actors only have modest ambitions, however, they will be more willing to settle for less and to employ less effective modes of operation. Voluntary limitation of means enables an aggressor to minimize both costs and risk exposure. The voluntary limitation of ends allows the target to keep more of what it already has. Escalation in this situation is thus mutually undesirable. In order to limit the risk of escalation, gray zone actors voluntarily limit the means they use to pursue their limited ends.

The Iraq War illustrates all four categories. The U.S.-led Coalition invaded Iraq in 2003 with less than 180,000 troops even though the United States could have, and the U.S. Army wanted to, mobilize hundreds of thousands more. Major combat operations in Iraq were limited by a desire to cut costs, not concerns about deterrence. As subsequent events made clear, American politicians ignored the significant and arguably foreseeable costs of occupation.[46] Throughout the next decade the U.S. military battled a mixture of foreign jihadists and local militias. While insurgent groups used similar means—improvised explosive devices and ambush attacks—their aims differed. Jihadists sought the revolutionary transformation of Iraqi society. Militias sought to control local areas and economies. Coalition Forces struggled with both groups before learning how to defeat the former (with the counterterrorism methods of Joint Special Operations Command) and to coopt the latter (by striking deals with the Anbar Awakening and similar movements).[47]

Had American policymakers appreciated the true costs of their war, they would have faced a choice between two alternatives. If they were indeed resolved to conquer Iraq, they could have increased force levels to enable both invasion and stabilization. That is, they could have conducted major combat operations with a larger set of means and resources. The troop surge of 2008 followed a similar logic by increasing resources in an attempt to transform Iraq into a stable liberal society. If, however, policymakers' war aims were more limited, as they arguably should have been, they might have sought an alternative to invasion, such as maintenance of the existing containment regime. Indeed, between 1991 and 2003, the United States engaged in a continuous gray zone contest to contain Saddam Hussein with air policing, economic sanctions, covert intelligence, and occasional air strikes. The Baathist regime survived while the United States avoided a costly ground war, outcomes that were mutually preferable for both sides compared to the, at that time anticipated outcome of the

[46] and counterinsurgency in Iraq Risa Brooks, *Shaping Strategy: The Civil-Military Politics of Strategic Assessment* (Princeton, NJ: Princeton University Press, 2008), 226–55; Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (Ithaca, NY: Cornell University Press, 2011), 137–84.

[47] Michael R. Gordon and Bernard E. Trainor, *Cobra II: The Inside Story of the Invasion And Occupation of Iraq* (New York: Vintage Books, 2007); Michael R. Gordon and Bernard E. Trainor, *The Endgame: The Inside Story of the Struggle for Iraq, from George W. Bush to Barack Obama* (Pantheon Books, 2012); Jon R. Lindsay and Roger Petersen, "Varieties of Insurgency and Counterinsurgency in Iraq, 2003-2009," Center for Irregular Warfare and Armed Groups Case Study Series (Newport, RI: Naval War College, 2012); Sean Naylor, *Relentless Strike: The Secret History of Joint Special Operations Command* (St. Martin's Press, 2015).

war. Intelligence assessment and rational decision making are each important for assessing the parameters of deterrence, and both proved defective in this case.[48]

As the Iraq case highlights, the distinction we present above (as depicted in Table 1) is often less stark in practice. Gray zone conflict is not just a matter of limited ends but also, and primarily, of risk-sensitivity. In both categories of limited conflict (gray zone and major combat), strong actors choose to limit means, but they do so for different reasons. A resolved actor that values the stakes of the conflict may be willing to pay more to get a better outcome. But it does not necessarily have to have a favorable balance of power; it may want to spend its surplus on other domestic projects, for instance. A less resolved actor, however, will not want to risk paying more and will be willing to compromise to avoid doing so. The fact that both types pull their punches creates something of a "gray zone" between our two categories.

The Escalation Dilemma

Given that capable actors may use limited means for limited ends for quite different reasons, the label of "major combat operations" is a rather misleading way to describe conflict motivated by efficiency.[49] A challenger who is patient and capable relative to its adversaries at low intensities might benefit by choosing a limited conflict strategy. While high intensity conflict may be able to accomplish an aggressor's goals, it may also be unnecessary and inefficient if victory can be achieved with lower cost at lower levels of dispute intensity.[50] If the local balance of power greatly favors the initiator, then it may only need to employ modest resources to get all that it seeks in a reasonable timeframe. If the aggressor only needs a few special operations units and some cyber effects to overwhelm the enemy, then a contest may be observably indistinguishable from the prototypical gray zone conflict. This sort of indistinguishability is most likely in cases where the revisionist actor has limited aims but values them greatly, i.e., it desires something well short of total conquest and only needs to mobilize a small number of forces to compel the other side to make concessions.

Escalation becomes the distinguishing test that separates gray zone conflict and major combat operations. By raising the cost of gray zone conflict, defenders can force the initiator into fighting less efficiently, but only by also accepting higher costs/risks themselves, something that may be mutually unappealing. Threats of retaliation or actual military resistance may cause an influence-maximizing combatant to switch to a more efficient, and more intense, form of combat. This type of actor prefers high intensity warfare to ordinary peacetime competition. The risk-sensitive gray zone actor, by contrast, will back down in the

[48] The U.S. invasion of Iraq was prompted by pessimism about efforts in the gray zone, and an exogenous shock in the form of the 911 terrorist attacks. In other words, the desire for gray zone was no longer mutual.

[49] Conversely, as the Iraq case illustrates, "gray zone" is a poor description of cases where actors fail to exercise restraint because they do not understand their own deterrence sensitivities.

[50] Altman, "Advancing without Attacking."

face of robust resistance, accepting both inefficiency and ineffectiveness. This actor prefers peacetime competition to major war. These preference orderings can be summarized thus:

$$\text{Limited conflict} \gtrsim \text{Ordinary competition} \gtrsim \text{High intensity warfare}$$

$$\text{Limited conflict} \gtrsim \text{High intensity warfare} \gtrsim \text{Ordinary competition}$$

Behaviorally both types of conflict look like they are in the gray zone. However, each displays different escalation dynamics. An actor with the first set of preferences should escalate if opposed, preferring war to peace, while an actor with the second preference ordering will tend to back down, preferring peace to war. The first type of actor is motivated by efficiency. It is willing to go to war to achieve its objective, but limited conflict is easier and/or lower cost. The second type is constrained by deterrence. Retaliation or related consequences (incursions, sanctions, etc.) that result from its ambiguous use of force are seen as sufficiently costly that the initiator refrains from pursuing them, or conducts them more ineffectively simply to save face. This situation might be described as pure gray zone conflict as discussed above in the typology of Table 1. The former situation, by contrast, is a mixed or behavioral form of gray zone conflict. A pressing challenge for the target of limited aggression is how to glean the aggressor's valuation of the stakes and willingness to run risks to achieve them.

This situation recapitulates the basic logic of the security dilemma [51]. The classic problem is to divine whether a state is satisfied with the status quo or has revisionist intentions. The spiral model applies to the former while the deterrence model applies to the latter; applying the wrong model leads to tragic escalation (threatening status quo seekers) or preventable exploitation (appeasing revisionists). The difference here is that the gray zone actor is already known to be revisionist; the uncertainty is thus more about its resolve than its interest. In security dilemma logic, escalation occurs when the deterrence model is (inappropriately) applied to a status quo actor (but not to the revisionist). In gray zone logic, escalation occurs when the deterrence model is applied to a more resolved revisionist (but not to the less resolved aggressor). If the problem of the security dilemma is to decide *whether* to deter, the problem of the gray zone is to decide *how much*. Even if all actors are assumed to harbor revisionist ambitions [52], security dilemma-like dynamics still apply in determining the ways in which they are deterred from given behavior.

The Deterrence Gradient

If conflict varies continuously between peace and war, then if might be explained by treating deterrence success and failure as also variable. If gray zone conflict is a second-best reaction

[51] Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (1978): 167–214; Shiping Tang, "The Security Dilemma: A Conceptual Analysis," *Security Studies* 18, no. 3 (2009): 587–623.

[52] Randall L. Schweller, "Neorealism's Status-quo Bias: What Security Dilemma?," *Security Studies* 5, no. 3 (March 1, 1996): 90–121, https://doi.org/10.1080/09636419608429277.

to successful deterrence, then conflict severity should be inversely proportional to the credibility of deterrence. Conflict motivated by efficiency should not be so correlated. Furthermore, conflict at the weaker end of the deterrence gradient should be more motivated by efficiency concerns than fears about retaliatory consequences.

To operationalize this hypothesis, we posit a deterrence analogue to the military loss of strength gradient.[53] All things being equal, a state requires more supplies and troops to achieve the same concentration of force further from its border. Distant deployments involve extended supply lines and exposed flanks. An army may also lack sympathetic populations and local knowledge in "contested zones" far from home.[54] The loss of strength can be partially offset by basing and mobility but not eliminated due to the enduring vulnerabilities of naval power and frictions with host nations.[55] Geography is not the focus of this article, per se, but we use it here to instrument variation in the strength of deterrence. This in turn enables us to examine arguments about the relationship between deterrence and gray zone conflict. We do not assume that geography causes deterrence directly, but it can be used as an adequate and convenient proxy for other factors that do.

Insofar as military power is affected by a loss of strength gradient, deterrence that relies on military power should also decay in distance. There are other reasons to expect resolve to be affected by proximity. All things being equal, states likely care more about regional issues that more directly affect their populations than about happenings far from home. Defenders will thus be more resolved to resist aggression on their borders, while attackers campaigning from distant shores will are less so. Alliances with neighboring states should similarly be more credible since patrons are generally more willing to defend a proximate client.[56] Conversely, commitments should be less credible with distance as well, as patrons will fear entrapment by distant allies with stronger local interests [57]. Extended deterrence—the use of threats to protect allies beyond a state's borders—is thus widely believed to be less credible than homeland deterrence.[58] The NATO solution to this problem has been forward deployment of U.S. forces.

Alliance commitments are to extended deterrence what forward basing is to the loss-of-strength gradient; both mechanisms seek to roll back the damaging effects of distance. Just

[53] Boulding, *Conflict and Defense*.

[54] Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* 28, no. 1 (July 1, 2003): 5–46, https://doi.org/10.1162/016228803322427965; Erik Gartzke and Patrick Hulme, "The Tyranny of Distance: Assessing and Explaining the Apparent Decline in U.S. Military Performance" (Manuscript, June 2019).

[55] Julian Corbett, *Some Principles of Maritime Strategy* (Longmans, Green and Co., 1911); Norman Friedman, *Seapower as Strategy: Navies and National Interests* (Naval Institute Press, 2001).

[56] Daehee Bak, "Alliance Proximity and Effectiveness of Extended Deterrence," *International Interactions* 44, no. 1 (January 2, 2018): 107–31, https://doi.org/10.1080/03050629.2017.1320995.

[57] Thomas J. Christensen and Jack Snyder, "Chain Gangs and Passed Bucks: Predicting Alliance Patterns in Multipolarity," *International Organization* 44, no. 02 (March 1990): 137–168, https://doi.org/10.1017/S0020818300035232.

[58] Matthew Fuhrmann, "On Extended Nuclear Deterrence," *Diplomacy & Statecraft* 29, no. 1 (January 2, 2018): 51–73, https://doi.org/10.1080/09592296.2017.1420526.

as not all outposts are created equal, furthermore, some commitments are stronger than others. While NATO security guarantees nominally cover all 29 member states equally, the 12 founding members in Western Europe and North America are arguably more confident in this commitment.[59] Indeed, recent Eastern European entrants have questioned NATO resolve. Declarations that there is no second tier in NATO simply underscore this concern. Eastern European members also appear to have greater need of protection, given that Russia is both more interested in, and better able to, control territory near its borders.[60] In sum, Western resolve and capability decreases from West to East while Russian resolve and capability increases.

Technology conditions but does not eliminate geography. Cyberspace seems to open up the entire world to anyone with an internet connection. Yet most states can and do enforce their laws on the digital infrastructure within their borders, which they connect across borders for good economic reasons.[61] The terrestrial metaphor of "cyberspace" elides the mutual interests actors have in building and maintaining the sociotechnical institutions that enable them to share information and make money.[62] What happens in the cyber domain is conditioned by the power and interests of actors in other domains. Indeed, cyber conflict appears to be concentrated along the fissures of traditional geographic rivalries.[63]

To the extent that cyberspace does enable remote conflict, we should expect it to be used for limited aims operations that do not directly threaten vital interests. Because cyber-attacks rarely lead to escalation, the cyber domain is particularly attractive for risk-sensitive revisionists.[64] Similarly, navies have traditionally been useful for limited war because they could raid an adversary's distant assets without directly threatening its homeland.[65] The cybersecurity literature offers two logics for the empirical pattern of restraint observed in

[59] Justin George and Todd Sandler, "Demand for Military Spending in NATO, 1968–2015: A Spatial Panel Approach," *European Journal of Political Economy* 53 (July 1, 2018): 222–36, https://doi.org/10.1016/j.ejpoleco.2017.09.002.

[60] Timo Noetzel and Benjamin Schreer, "NATO's Vietnam? Afghanistan and the Future of the Atlantic Alliance," *Contemporary Security Policy* 30, no. 3 (December 1, 2009): 529–47, https://doi.org/10.1080/13523260903327618; Janne Haaland Matláry, "Partners versus Members? NATO as an Arena for Coalitions," in *NATO's Post-Cold War Politics: The Changing Provision of Security*, ed. Sebastian Mayer, New Security Challenges Series (London: Palgrave Macmillan UK, 2014), 251–66, https://doi.org/10.1057/9781137330307_14.

[61] Daniel W. Drezner, "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly* 119, no. 3 (2004): 477–98, https://doi.org/10.2307/20202392; Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford University Press, 2006).

[62] Mark Raymond, "Puncturing the Myth of the Internet as a Commons," 2013; Jesse H. Sowell, "Finding Order in a Contentious Internet" (Thesis, Massachusetts Institute of Technology, 2015), http://dspace.mit.edu/handle/1721.1/97324; Jon R. Lindsay, "Restrained by Design: The Political Economy of Cybersecurity," *Digital Policy, Regulation and Governance* 19, no. 6 (July 26, 2017): 493–514, https://doi.org/10.1108/DPRG-05-2017-0023; Jordan Branch, "Spatial Metaphors and the Territorialization of Cybersecurity" (International Studies Association Annual Conference, San Francisco, CA, 2018).

[63] Brandon Valeriano and Ryan Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," *Journal of Peace Research* 51, no. 3 (May 2014): 347–60.

[64] Jacquelyn Schneider, *The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict* (ProQuest LLC, 2017).

[65] Corbett, *Some Principles of Maritime Strategy*.

the cyber domain, and geography plays a tacit role in both.[66] First, complex offensive cyber operations require detailed intelligence preparation, often including human intelligence.[67] It is noteworthy that the United States relied on a regional partner (Israel) for the Stuxnet operation. Intelligence is harder to collect and understand from a distance, and poor intelligence enhances cyber deterrence-by-denial. Second, attribution and retaliation depend on capabilities in more traditional domains.[68] Thus deterrence-by-punishment of cyber aggression will be affected by the same deterrence gradient that affects cross-domain military capabilities in the terrestrial world.

A Note on Third Parties

As the logic of our argument is dyadic, the role of third parties deserves a brief comment. Many treatments of covert warfare focus on military aid to local proxies from a powerful patron. As an analytical first cut, a complex portfolio of actors can be simplified as a dyadic pairing in gray zone conflict.[69] That is, a target's allies can be treated as part of the target's capabilities, discounted by the level of commitment (or disunity) in an alliance. Lanoszka argues that a gray zone initiator must have escalation dominance over the target, e.g., Russia has more capability at every rung of the escalation ladder than Ukraine or Lithuania.[70] His argument seems to run counter to our deterrence story until the weaker state is combined with its powerful protector(s). Russia may not be deterred by the Ukrainian military directly, but it calibrates its actions to avoid triggering a confrontation with NATO. More actors should thus be considered "capable" than if assessed in purely bilateral terms.

Importantly, alliances, commitment mechanisms, and other attempts to aggregate capabilities are often explicitly or implicitly designed to generate deterrence by reducing agency (autonomy) on the part of individual participants, making them behave more like a

[66] Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011."

[67] Jon R. Lindsay, "Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations," *Journal of Strategic Studies* 36, no. 3 (June 1, 2013): 422–53, https://doi.org/10.1080/01402390.2012.734252; Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (April 3, 2015): 316–48, https://doi.org/10.1080/09636412.2015.1038188; Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford University Press, 2016); Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (January 1, 2017): 72–109, https://doi.org/10.1162/ISEC_a_00267.

[68] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (October 1, 2013): 41–73, https://doi.org/10.1162/ISEC_a_00136; Gartzke and Lindsay, "Weaving Tangled Webs"; Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (July 3, 2017): 452–81, https://doi.org/10.1080/09636412.2017.1306396; Jacquelyn Schneider, "Deterrence in and through Cyberspace," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Jon R. Lindsay and Erik Gartzke, 1st edition (New York, NY: Oxford University Press, 2019).

[69] At least initially. For complications, see Timothy W. Crawford, *Pivotal Deterrence: Third-Party Statecraft and the Pursuit of Peace* (Cornell University Press, 2003); Wendy Pearlman and Boaz Atzili, *Triadic Coercion: Israel's Targeting of States That Host Nonstate Actors* (New York: Columbia University Press, 2018).

[70] Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe."

single unit.[71] Deterrence works if an ally might respond to a given provocation, but friction between them complicates deterrence effectiveness.[72] Indeed, misalignment of interests within an alliance (or domestic civil politics) can serve to weaken deterrence and provide opportunities for gray zone intervention.

Conflict initiators can similarly rely on proxies to complicate the deterrence calculus. Ambiguity regarding responsibility for an attack makes a retaliatory response less likely, especially if the target is looking for reasons not to retaliate.[73] Recognizing the potential for agency problems, targets may discount the harm that proxies inflict. Reliance on third-parties may thus transform cases that would have been small wars into gray zone conflicts. The explicit delineation of an extended deterrence *quid pro quo* probably increases this risk, as red lines clarify what can be achieved in the gray zone.

Russian Gray Zone Campaigns

We now test the plausibility of our argument about deterrence sensitivity by examining major Russian foreign interventions over the past two decades. Almost all cases feature cyber campaigns for disruption or influence. Some also feature intervention by special operations or conventional forces. Why does Russia bring more of its capabilities to some fights than others? We focus on Russia because its recent interventions, especially those featuring significant cyber operations, are often referenced as paradigmatic examples of gray zone conflict.[74] Specifically, we focus on four major Russian cyber campaigns targeting states that are geographically situated at different locations along the Western deterrence gradient: Estonia (2007), Georgia (2008), Ukraine (2014), and the United States (2016). The diversity of Russian targets provides an opportunity to conduct a natural controlled comparison of Russian choices under different deterrent circumstances.

Cross-National Data

It is perhaps fitting that data on Russian gray zone interventions are themselves ambiguous. Previous studies have compiled open source data on Russian-attributed cyber conflict over the past three decades. Two cross-national datasets – Dyadic Cyber Incident and Dispute V1.1 (DCID) and Russian Electoral Interventions (REI) – cover almost entirely distinct samples.[75] Indeed, the only country-year that appears in both datasets is Ukraine 2014. The

[71] David Sobek and Joe Clare, "Me, Myself, and Allies: Understanding the External Sources of Power," *Journal of Peace Research* 50, no. 4 (July 1, 2013): 469–78, https://doi.org/10.1177/0022343313484047.

[72] Vesna Danilovic, "The Sources of Threat Credibility in Extended Deterrence," *Journal of Conflict Resolution* 45, no. 3 (June 1, 2001): 341–69, https://doi.org/10.1177/0022002701045003005.

[73] Borghard and Lonergan, "The Logic of Coercion in Cyberspace."

[74] Freedman, "Ukraine and the Art of Limited War"; Marten, "Putin's Choices"; Driscoll and Maliniak, "With Friends Like These"; Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe"; Chivvis, "Hybrid War."

[75] Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011"; Adam Casey and Lucan Ahmad Way, "Russian Electoral Interventions, 1991-2017" (Scholars Portal Dataverse, 2017), https://doi.org/10.5683/SP/BYRQQS. Data by Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital

DCID data identifies the United States, United Kingdom, Poland and Ukraine as targets of the most severe Russian cyber operations. In the cases documented by REI, the most severe Russian attacks occurred against France, Austria, and Ukraine. The different emphases of each dataset result in major coding heterogeneity.

We present an expanded and consolidated dataset of 82 cases of Russian intervention from 1994-2018.[76] DCID and REI together describe 71 unique cases of Russian aggression that have either included some degree of cyber intervention or were cases of electoral interference. We have identified 10 additional instances of Russian cyber-attacks from 1994-2018 and also include 3 cases of non-cyber Russian aggression during this time period from the International Crisis Behavior (ICB) dataset.[77] Including ICB data has the further advantage of not focusing exclusively on Russian cyber-attacks but also including all Russian conflict short of war. To resolve the heterogeneity across datasets, we compiled an entirely new coding of the intensity of Russian attacks. For each incident, we code whether Russia used conventional ground forces, conventional air or sea forces, paramilitary or covert forces, cyber disruption (service denial or industrial control system attacks), and information operations (social media and disinformation). By distinguishing between these five types of aggression, we obtain a clearer picture of the intensity of each case of Russian intervention.

Figure 1 shows the frequency distribution of Russian gray zone operations since 1994. Contrary to descriptions of gray zone conflict as new or the product of new technologies of war, there does not appear to be an increase in low-intensity or non-kinetic Russian activity over time. Chechnya (1999) and Georgia (2008) represent the most intense Russian intervention and 2014 experienced the highest number of interventions (most of which were associated with Ukraine). Russian gray zone operations have not increased in intensity, but they do appear to be happening more frequently. This might reflect a weakening of Western deterrence, an emboldening of Russian leadership, or the maturation of technical capabilities. Whatever the cause, the result is likely to be a self-defeating (for Russia) strengthening of Western defenses and resolve given better information about the nature of the Russian threat. Like a stain on a microscope slide, Russian operations highlight the contours of the Western deterrence gradient.

A basic hypothesis of our theory is that limited war constrained by deterrence (gray zone conflict) should be distributed along a deterrence gradient, with conflict intensity inversely proportional to the credibility of deterrence. Limited war that is motivated by efficiency, by contrast, should be less correlated with geography.

Front: Can Cyber Attacks Shape Battlefield Events?," *Journal of Conflict Resolution* 63, no. 2 (2019): 317–47, https://doi.org/10.1177/0022002717737138 is too narrowly focused on cyber-attacks in Ukraine.

[76] Our unit of analysis is country-year. See the data appendix to this article for further discussion.

[77] David J Singer, Stuart Bremer, and John Stuckey, "Capability Distribution, Uncertainty, and Major Power War, 1820-1965," in *Peace, War, and Numbers*, by Bruce M. Russett (Sage Publications, 1972), 19–48.

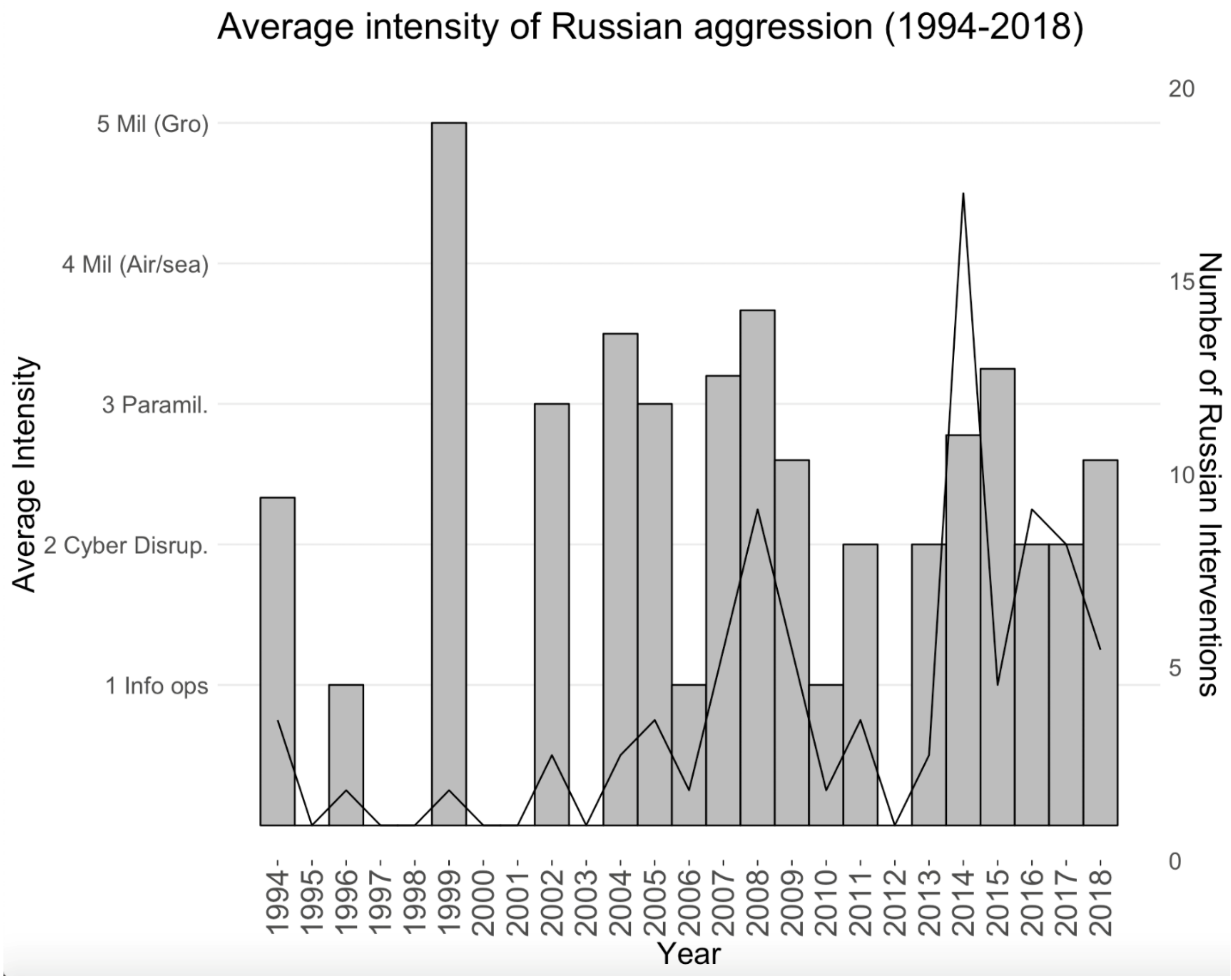

Figure 1 *Intensity of Russian intervention over time. The bars represent the average intensity of Russian interventions in each year using the 1-5 scale provided. The line denotes the number of Russian interventions in each year..*

Figure 2 reveals a pattern that is roughly consistent with our argument about the geographical deterrence gradient. At the West end is the United States, and on the East end is Russia. In between are European states in a variety of alliance configurations with the United States, to include no alliance at all. Russia appears to be willing to use more force in its “near abroad” (where it is less deterred) than farther away. The exception to this geographical pattern is in Syria, which hosts a major Russian naval base on the Mediterranean. The port of Tartus, a staging base for Russian combat operations in Syria, serves to lessen the Russian loss of strength gradient and may help to explain the Syrian exception to the East-West pattern in the intensity of Russian operations in Figure 2.

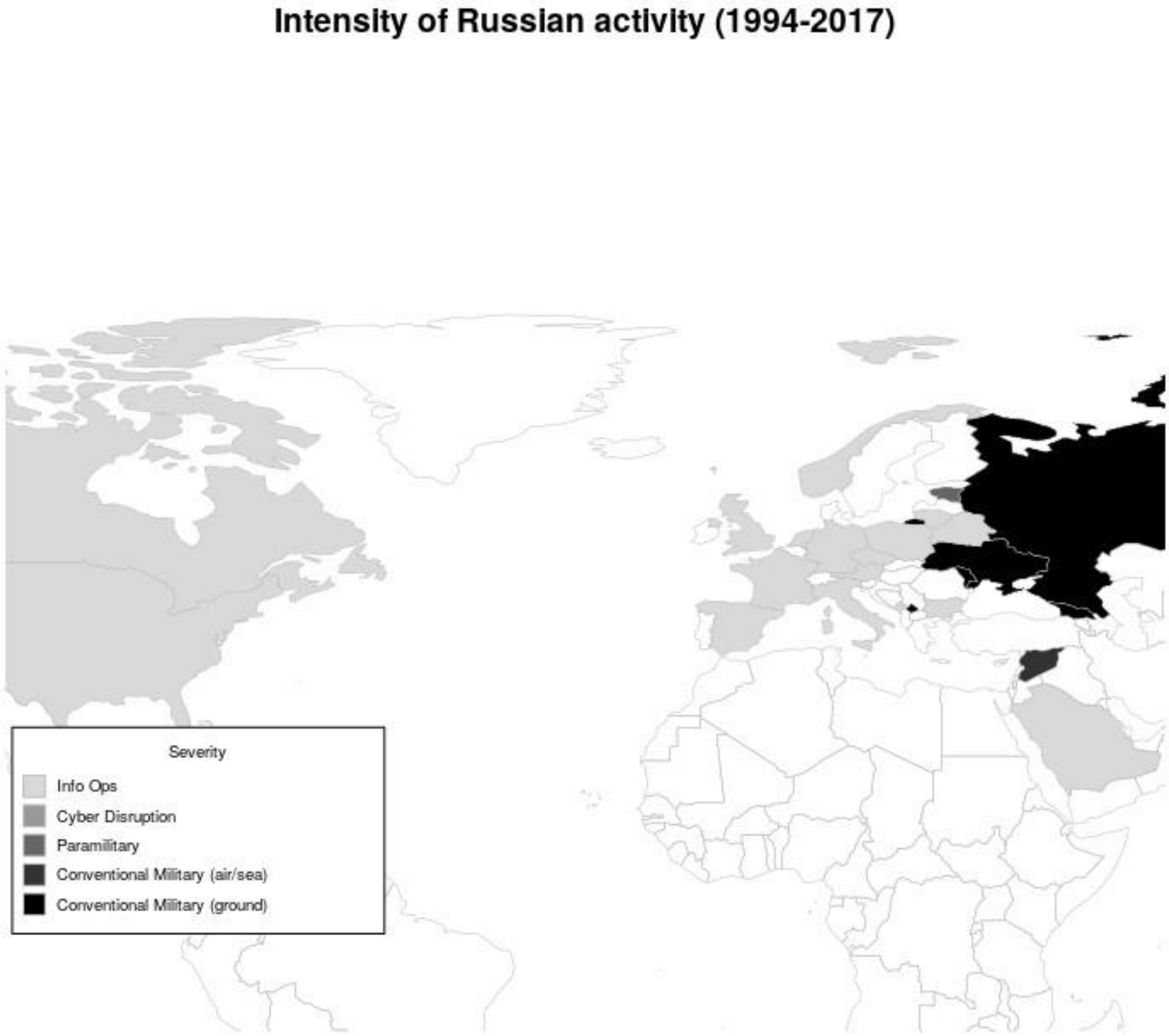
Intensity of Russian activity (1994-2017)
Severity
Info Ops
Cyber Disruption
Paramilitary
Conventional Military (air/sea)
Conventional Military (ground)

Figure 2 *Geographic representation of Russia intervention. Each country's shading represents the highest intensity of Russian intervention in that state between 1994-2017. States closer to Russia have noticeably higher levels of severity.*

Because the deterrence gradient still matters in cyberspace, furthermore, we see Russia conducting low-intensity cyber influence and espionage operations around the world, while it conducts high-intensity cyber-physical operations in closer proximity to its border. While Russian influence operations are ubiquitous, cyber disruption is less common, and overt military intervention occurs only in Russia's immediate periphery ("near abroad").

Major Cyber Campaigns

Russia is involved in numerous gray zone conflicts, but the actual shade of gray in each case depends on the deterrence gradient. For a more fine-grained test of our argument, we briefly examine the four major cyber campaigns attributed to Russia that feature prominently in the cybersecurity literature. The usual focus on cyber operations themselves tends to obscure the cross-domain and cross-national context of these operations. We employ a most similar case comparison by choosing cases that have the same conflict initiator (Russia) and the same means of low intensity conflict (cyber) but that differ in their geographical location and other military instruments employed.[78] We code four rough categories of Russian operations in declining level of intensity, risk, and cost for the initiator (Russia): overt deployments of conventional military force, covert use of special operations or unattributed military forces, cyber operations that result in disruption of infrastructure, and information operations.

We do not focus here on the origins of Russian motives or their formulation in Russian foreign policy, even as understanding these is essential for devising practical policy responses in any given case. There are many potential explanations for Russian motives, to include the personality of Vladimir Putin, political competition for regime control, nationalist identity and status seeking, and geopolitical imperatives for security.[79] Rather we argue that how motives are expressed, whatever their origins, will be more or less constrained by Western deterrence. We will consider some counterarguments in the case narratives.

Table 2: Case comparison of Russian gray zone conflicts

Russian Response	United States (2016)	Estonia (2007)	Ukraine (2014)	Georgia (2008)
Conventional Forces				X
Special Operations			X	X
Disruptive Cyber		X	X	X
Information Operations	X	X	X	X

Table 2 lists these cases by distance from Washington DC.[80] Again the geographical pattern is striking. Moscow is more likely to pull its punches for cases closer to Washington. While geography is simply a proxy for other factors that condition the strength of Western deterrence, these factors combine to create a gradient of decreasing deterrence. Russian operations directly against the United States are limited to cyber influence and espionage

[78] Andrew Bennett and Colin Elman, "Case Study Methods in the International Relations Subfield," *Comparative Political Studies* 40, no. 2 (February 2007): 170–95, https://doi.org/10.1177/0010414006296346.

[79] Driscoll and Maliniak, "With Friends Like These"; Elias Götz, "Putin, the State, and War: The Causes of Russia's Near Abroad Assertion Revisited," *International Studies Review* 19, no. 2 (June 1, 2017): 228–53, https://doi.org/10.1093/isr/viw009.

[80] We considered other geographic measures of the deterrence gradient like distance from Moscow or contiguity with Russia. We found less variation on these measures given half of the cases border Russia (Georgia, Ukraine, and Estonia) and one (Chechnya) occurred within Russia's borders. Distance *from* the United States is also more in keeping with the loss of strength gradient for retaliations initiated by the United States.

operations. Operations against Estonia are still restrained—given its membership in NATO—but also include a punishing wave of DDoS attacks. Ukraine is not a member of NATO and is highly salient to Russia, but it borders European NATO states and was in negotiation for EU membership when the crisis began. Russian attacks are diverse but fall short of overt, avowed military intervention. Georgia is not a NATO member and is deep in Russia's sphere of influence. At the weakest end of the deterrence gradient, Russia intervened in Georgia using not only cyber-attacks but also paramilitaries and overt military force.[81]

Estonia (2007)

A signal event in the brief history of cyber conflict was the 2007 DDoS attack that roiled Estonia. It was precipitated by the relocation of a Soviet-era statue from the center of Tallinn to its outskirts, which sparked rioting by the Russian minority resulting in injuries and one death. That evening internet traffic surged beyond average peak loads by a factor of ten or more and degraded the availability of government, media, and banking websites and cash machines. "The most wired country in Europe" was uniquely dependent on online transactions, and no country, let alone a NATO member, had ever been attacked so suddenly and aggressively by a botnet.[82] Estonia's defense minister considered but ultimately rejected invoking Article V, the collective defense clause of the NATO treaty, instead requesting and receiving technical assistance.[83] The attacks continued in attenuated form for two and a half weeks. Some ambiguity about responsibility persists, but evidence suggests coordination from the Russian government in collaboration with so-called patriotic hackers.[84]

The 2007 campaign reflects a cautious Russian effort in the gray zone, which was not only conditioned by NATO's general deterrence posture but also enabled by its ambiguity. Estonia, a former Soviet republic, had joined NATO in 2004 over Russian objections. The gap in time between NATO ascension and the Russian cyber campaign is telling; in Georgia and Ukraine the mere prospect of future NATO membership contributed to the crisis. Russia acted to register a grievance and test NATO responses, not to defend a vital interest. The Estonian attacks were more of an opportunistic protest rather than a determined bid to change (or return) the status quo, although tools had been prepared for patriotic hackers prior to the removal of the statue in anticipation of just such an opportunity. All sides—the belligerents, their agents, their targets, and external audiences—were relatively inexperienced with cyber operations at scale in 2007. The legal status of a cyber-attack had

[81] Although not considered in detail here, Russian operations in outside cases like Kosovo and Chechnya are consistent with the deterrence gradient.

[82] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/.

[83] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 17, 2007, sec. World news, https://www.theguardian.com/world/2007/may/17/topstories3.russia.

[84] Andreas Schmidt, "The Estonian Cyberattacks," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, ed. Jason Healey (Cyber Conflict Studies Association, 2013), 174–93.

not yet been clarified, which provided both an opportunity and a constraint for Russia.[85] NATO would be unlikely to seriously consider formally responding so long as Russia avoided causing serious harm. Estonia ultimately treated the incident as a law enforcement matter, arresting a teenaged hacker in Tallinn. The tacit agreement between adversaries to limit the scope of conflict and obfuscate responsibility to avoid escalation echoes the logic of covert confrontation in the Cold War.[86]

As an exercise in coercion, the Russian campaign was ultimately a failure. No one issued any clear demands or claimed responsibility. Estonia did not replace the statue. After the event, Tallinn became more resolved to bind with the West. Indeed, Estonia has become a hub for coordinating NATO cyber defenses. The Estonian event, like most DDoS attacks, amounted to an ambiguous symbolic outburst which created financial costs and inconvenience for the target. Such acts may tell you that someone is upset, but they also tell you that someone is not upset or confident enough to really do something about it.

Georgia (2008)

A year later, Georgia was hit by similar waves of DDoS attacks amidst an even more fractious duel of competing narratives in online fora.[87] Yet whereas the Estonian episode was restricted to the cyber domain, Russia also intervened militarily in Georgia, an early example of cross-domain operations leveraging cyberspace. While cyber-attacks did not directly affect tactical operations, they did interfere with government coordination and financial infrastructure. Official and non-official sources on both sides also waged vigorous media campaigns to represent the war alternatively as a humanitarian intervention (with legal precedent in NATO's mission in Kosovo) or a war of Russian aggression.

Following the civil war after the Soviet collapse, Russia stationed peacekeepers in Abkhazia and South Ossetia, ostensibly to protect non-Georgian minorities. Tbilisi resented the occupation and, especially after the Rose Revolution of 2003, sought Western security guarantees and NATO membership.[88] NATO, for its part, encouraged Georgia (and Ukraine) to apply for membership in the April 2008 Bucharest Summit Declaration. The same month Russia announced that it would unilaterally increase peacekeepers in Abkhazia. Terrorist bombings in South Ossetia provoked Tbilisi to mobilize in August, which prompted Russia to invade South Ossetia and establish a naval blockade on the Abkhaz coast. The Russian military defeated Georgian forces after five days of heavy fighting, and the two sides signed

[85] Vincent Joubert, "Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?" (NATO Defense College, 2012), JSTOR, https://www.jstor.org/stable/resrep10366.

[86] Carson, *Secret Wars*.

[87] Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (February 1, 2012): 3–24, https://doi.org/10.1177/0967010611431079.

[88] Driscoll and Maliniak, "With Friends Like These."

a peace agreement on 15 August which left Russian forces stationed in the de facto autonomous provinces.[89]

Russia's intervention choices in this conflict, situated at the far end of the Western deterrence gradient, were more motivated by efficiency than deterrence. Russia used whatever mix of tools it needed to accomplish its objective and did not appear to pull its punches out of concern for Western counteraction. If anyone was deterred, it was NATO. As Driscoll and Maliniak point out, "because of Georgia's location and its contested map, it is a security liability from the point of view of many in the West."[90] Despite the optimism of the Bucharest Declaration, NATO membership or armed assistance was never a realistic option. The extension of Article V would have encouraged moral hazard, given Tbilisi's perception of Russian peacekeepers as an illegal occupation, and NATO states would have been hard pressed to honor that insurance policy. The Russian intervention served to clarify the stakes of Western interference in its near abroad. While Russia's tactical performance left much to be desired, the mission was a strategic success that reinforced the status quo ante and ended the conversation about Georgia joining NATO. Our theory predicts that a Western response that raised the cost of conflict for Russia would have only escalated the situation since Russia's actions were chosen not out of fear of escalation, but through a calculation that its objectives could be accomplished at reasonable cost. The "frozen conflict" in Georgia also anticipated the emergence of similar militarized standoffs in Eastern Ukraine.

Ukraine (2014)

One might argue that Russia values the stakes differently in each conflict and thus the correlation with the deterrence gradient observed in Table 2 is spurious. The cases of Estonia and Georgia appear to be consistent with this alternative explanation. Russia let Estonia join NATO without a fight in 2004 and merely sought to register a protest vote in 2007 when Tallinn moved a Soviet statue. By contrast, Russia had supported separatists in Georgia since the early 1990s and was highly resolved to ward off Western encroachment. Efficiency alone might thus explain the single-domain response in Estonia versus the multi-domain engagement in Georgia. The Ukraine case, however, finds this alternative account wanting.

Ukraine, seat of the medieval Kievan Rus empire, is more salient in Russian nationalist mythology than Georgia, a peripheral outpost in the Caucuses far from Moscow. Russian identify, aspiration, and resentment has always looked toward Europe, not Asia. The Black Sea port of Sevastopol also makes Crimea more strategically relevant. Russian military planners have long expressed more concern over NATO forward deployment in Ukraine than

[89] Paulo Shakarian, "The 2008 Russian Cyber Campaign against Georgia," *Military Review* 91, no. 6 (November 1, 2011): 63; Michael Brecher et al., "International Crisis Behavior Data Codebook," Codebook, 2017, http://sites.duke.edu/icbdata/data-collections/.

[90] Driscoll and Maliniak, "With Friends Like These."

in Georgia.[91] If Russian moves were motivated by efficiency rather than deterrence, then we would expect to see more overt Russian military efforts in Ukraine, as in Georgia. On the contrary, Russia took pains to create a fig leaf of ambiguity about the identity of Russian troops, the presence of Russian heavy weapons, and its role in orchestrating disinformation campaigns. There was never any real confusion about who was responsible for the "little green men" in Crimea, but the initial lack of consensus about whether Russia's actions violated international law created a pretext that enabled western powers to both uphold international law in principle and avoid any major action in practice.

The Western deterrence posture regarding Ukraine was weak, but it was also not nothing. The Western response in the wake of the Maidan crisis consisted mainly of economic sanctions, deployments of U.S. fighter jets to Poland, and eventually arms and assistance to Kiev, but no NATO ground combat forces on Ukrainian soil. Fighter jets would, of course, have been ideal for attacking Russian armored columns in a conventional war, but their very mobility made them a weak signal of commitment as compared to a counterfactual ground force deployment.[92] It is not uncommon in cross-domain deterrence that the means suited for winning one type of war are ill suited for deterring another type of war. This weakness created permissive conditions for Russian intervention. Nevertheless, NATO has conventional escalation dominance, should it decide to intervene on behalf of Ukraine. Russia would most likely lose a conventional contest involving NATO, risking escalation to nuclear war in the process. This risk has led to Russian circumspection. For example, when Malaysian Airlines flight MH17 was shot down over Donetsk by a Russian BUK anti-aircraft system, Moscow quickly withdrew all of its heavy weapons from the battlefield.[93] Gray zone conflict in Ukraine is implicitly shaped by Western deterrence, even though NATO has no formal commitment to Ukraine.

The cumulative intensity of the war in Ukraine has claimed a higher butcher's bill than the war in Georgia, consistent with higher Russian valuation of the stakes. The conflict in Georgia lasted only five days, but the conflict in Ukraine has dragged into its fifth year, resulting in nearly ten thousand killed and over a million displaced to date. Yet it is also notable that the protracted conflict has so far featured neither large scale combined arms warfare nor unrestrained ethnic cleansing or other human rights atrocities. Moreover, cumulative civilian deaths plateaued at about 4000 in 2015 while cumulative total deaths plateaued at about 9000 in 2016.[94] Covert interventions, even open secrets like Moscow's deployments

[91] Driscoll and Maliniak.

[92] Erik A. Gartzke and Koji Kagotani, "Being There: U.S. Troop Deployments, Force Posture and Alliance Reliability" (Working Paper, 2017).

[93] Laura Smith-Spark and James Masters, "Missile That Downed MH17 from 'Russian Brigade,'" *CNN*, May 24, 2018, https://edition.cnn.com/2018/05/24/europe/mh17-plane-netherlands-russia-intl/index.html.

[94] Jesse Driscoll and Zachary Steinert-Threlkeld, "Social Media and Russian Territorial Irredentism: Some Facts and a Conjecture" (Working Paper, 2019).

to Ukraine and aggressive cyber operations, tend to convey mixed signals of resolve and restraint.[95] The costliness of the intervention signals resolve, but the fact that costs could be higher and the efforts made to allow both sides to save face signals restraint. As Brantley et. al. points out, the modal diversity of conflict in Ukraine has lacked sufficient intensity to warrant outside intervention.[96]

The cyber domain is especially attractive for a risk-averse opportunist. Indeed, Ukraine has emerged as a testbed for Russian cyber warfare, even as Russia has not realized much for its efforts.[97] In the first major cyber-physical attack since Stuxnet, the Ukrainian power grid was briefly disrupted in 2015 and again in 2016, but services were quickly restored in each case.[98] These events were notable both for their technical sophistication and inconsequential strategic effects, not unlike Stuxnet.[99] NotPetya attacks, by contrast, may have wiped ten percent of the computers in Ukraine, including banks, federal agencies, and the Chernobyl clean-up site, and Maersk shipping worldwide was paralyzed for a few days via an infection in its Odessa office.[100] Yet the endemic Russian cyber-attacks and information operations have had little impact on battlefield events.[101] Even in social media operations, supposedly a devious Russian specialty, pro-Kremlin narratives never really took hold in Western Ukraine.[102]

United States (2016)

The most recent of the four major Russian cyber campaigns is both the most restrained and potentially most consequential. There is a general consensus that the Russian government interfered in the 2016 US election by hacking the Democratic National Committee, leaking incriminating information via Wikileaks, posting disinformation on social media sites like

[95] Carson, *Secret Wars*.

[96] Brantly, Cal, and Winkelstein, "Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW."

[97] Kenneth Geers, *Cyber War in Perspective: Russian Aggression against Ukraine* (CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015); Marie Baezner and Patrice Robin, "Cyber and Information Warfare in the Ukrainian Conflict," Report (ETH Zurich, June 2017), https://doi.org/10.3929/ethz-b-000169634; Brantly, Cal, and Winkelstein, "Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW"; Andy Greenberg, "How An Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

[98] Greenberg, "How An Entire Nation Became Russia's Test Lab for Cyberwar."

[99] Lindsay, "Reinventing the Revolution."

[100] NotPetya was a disk wiper malware disguised as ransomware (Petya) that exploited a National Security Agency (NSA) vulnerability called Eternal Blue. The White House estimates that global damages from NotPetya totaled $10 billion Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[101] Kostyuk and Zhukov, "Invisible Digital Front."

[102] Driscoll and Steinert-Threlkeld, "Social Media and Russian Territorial Irredentism: Some Facts and a Conjecture."

Facebook, and infiltrating lobbyist groups.[103] President Obama was aware of the Russian campaign in summer 2016 but did not publicly reveal his knowledge for fear of influencing the election.[104] A joint U.S. intelligence community statement was released soon after the election that concluded with "high confidence" that "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump."[105]

Within the scope of a covert election influence campaign, Russia did indeed pull out all the stops. This case is the exception that proves the rule that gray zone conflict is conditioned by deterrence. Moscow orchestrated a diverse suite of operations ranging from technical computer network exploitation and media influence operations to human intelligence.[106] Its full-court press could be described as unrestrained, even brazen, and thus motivated entirely by efficiency calculations. Yet the choice to pursue this course of action in the first place was very much constrained by the implicit deterrence posture of the United States. What else could Russia do? Russia could safely assume that the most powerful military in the world would retaliate for armed attacks directly against its vital interests. At the very least, American public opinion would thereby become more unified against Russia, resulting in policies more inimical to Moscow's interests. Non-kinetic covert action to subvert American institutions, however, offered a way for Russia to impose costs, potentially realize benefits, and minimize the risk of retaliation. Indeed, Russia's electoral interference has gone essentially unpunished by the United States to date, aside from the expulsion of some Russian intelligence officers and the application of a few sanctions in addition to the regime in place since 2014.

If Trump's victory or subsequent policies can ever be credited to active measures by the Russian Federation, even in part, it would amount to one of the most consequential

[103] Kimberly Marten, "Trump and Putin, Through a Glass Darkly," *Asia Policy* 23, no. 1 (February 10, 2017): 36–42, https://doi.org/10.1353/asp.2017.0005; Joshua Rovner et al., "Policy Roundtable 1-7: Russia and the 2016 U.S. Presidential Election," Policy Roundtable, H-Diplo ISSF, March 26, 2017, https://issforum.org/roundtables/policy/1-7-russia; Jensen, Valeriano, and Maness, "Fancy Bears and Digital Trolls"; Robert S. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," March 1, 2019, https://www.hsdl.org/?abstract&did=.

[104] David P. Fidler, "The U.S. Election Hacks, Cybersecurity, and International Law," *AJIL Unbound* 110 (ed 2016): 337–42, https://doi.org/10.1017/aju.2017.5.

[105] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community Assessment (Washington, DC: National Intelligence Council, January 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[106] Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency," Report for United States Senate Select Committee on Intelligence (New Knowledge, December 2018); Philip N Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018," Working Paper (Oxford, UK: Computational Propaganda Research Project, 2018); Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."

intelligence coups in history. It is just as likely that the Russian campaign simply added noise to one of the noisiest campaigns in U.S. presidential history. It is unclear how or even whether the Russian influence campaign affected voting behavior in what was, by any account, a very unique and chaotic election.[107] The Clinton campaign made its share of mistakes, and candidate Trump tapped into a deep and hitherto unexploited well of resentment in the American electorate.[108] Political context is ultimately more important than technical media for determining the effectiveness of information operations, and the fraught climate of 2016 was a perfect storm for opportunistic foreign influence. A slew of indictments and the final report by Special Counsel Robert S. Mueller III document collusion between the Russian government and members of the Trump campaign, even as questions remain about the extent of the candidate's personal involvement.

Discussion

The overall pattern of recent Russian intervention is largely consistent with our hypothesis that deterrence encourages capable actors to pull their punches. As the deterrence gradient drops off from West to East, Russia is more able to indulge in efficiency calculations in pursuing its international objectives. Again, geography does not determine deterrence, but it is correlated with other factors like military power, NATO membership, and the proximity of interests that shape deterrence credibility. The geographical correlation would not be present if conflict intensity were limited only by the means available to Russia or its calculations about the most efficient or effective way to conduct operations. While the degree of Russian interest does vary across these cases, the case of Ukraine in particular reveals that Russia is sensitive to deterrence even when its interests are high. Although Ukraine is strategically more important, Russian actions there were more constrained than in Georgia.

Differences in Russia's behavioral portfolio also cannot be explained through capability maturation alone or the availability of more options for conflict. The oldest cases (Estonia and Georgia) feature very different levels of intensity between them, as do the most recent (Ukraine and United States). To explain these differences, we must look to strategic incentives rather than technological capabilities. Gray zone conflict is not so much about the utilization of an expanding toolkit as careful decisions about what should be drawn from that toolkit.

One possible distinguishing difference of modern gray zone problems may be considered in terms of just what sort of deterrence actors are designing around. Previous studies have focused on adversaries who design around immediate deterrence, or threats issued in a crisis

[107] Andrew Gelman and Julia Azari, "19 Things We Learned from the 2016 Election," *Statistics and Public Policy* 4, no. 1 (January 1, 2017): 1–10, https://doi.org/10.1080/2330443X.2017.1356775.

[108] John Sides, Michael Tesler, and Lynn Vavreck, *Identity Crisis: The 2016 Presidential Campaign and the Battle for the Meaning of America* (Princeton, NJ: Princeton University Press, 2018).

situation; modern gray zone conflict often works to compromise general deterrence, or implicit barriers to crisis initiation.[109] Estonia or NATO did not issue a specific threat to Russia in 2007, but Russia had to take into account the possibility of Article V being invoked if it registered its protest too aggressively. The United States had not designated its electoral processes "critical infrastructure" to imply that cyber interference against them might be proscribed, but Russia still had to consider America's power to retaliate. The cyber domain, where general deterrence is unreliable and immediate deterrence works hardly at all, is well suited for just such subversion.[110]

Every Silver Lining's Got a Touch of Gray

Gray zone conflict occurs when capable actors intentionally limit the intensity or capacity of their aggressions and refrain from escalation. It differs from other forms of irregular or asymmetric warfare that are also limited because one of the combatants simply lacks the means to escalate the conflict. Unlimited war for a guerrilla will be limited war for the state. Gray zone actors, by contrast, pull their punches. We have argued that they do so out of concern for the potential consequences of their aggressions. Limited conflict, ironically enough, becomes a symptom of the success of deterrence. Gray zone conflict may be better understood as a reflection of weakness rather than an expression of strength.

While not new per se, gray zone conflict becomes more attractive with the expanding benefits of economic interdependence and cyber connectivity and the increasingly prohibitive cost of conventional, let alone nuclear, war. Though capable of acting more vigorously, powerful actors are deterred from initiating high-intensity conflict because of incentives to both cooperate explicitly through economic interdependence and coordinate tacitly for coexistence. Adversaries who no longer possess monolithic interests will also prefer to compete around the edges rather than openly confront opponents, concerned that the maximization of military power would undermine larger political objectives.

Just as there is a gray zone between war and peace, the distinction between effective and ineffective deterrence is also fuzzy. We have introduced the notion of the deterrence gradient, analogous to the military loss of strength gradient, to describe credible deterrence as a continuous variable. Wherever deterrence is credible (due to a favorable balance of power, greater relative valuation of the stakes, costly signals of commitment, a reputation for resolve, etc.), revisionists will exercise considerable restraint as they probe to see what they can get away with. Wherever deterrence is not credible, revisionists will be more

[109] Paul Huth and Bruce Russett, "Deterrence Failure and Crisis Escalation," *International Studies Quarterly* 32, no. 1 (1988): 29–45; Patrick M. Morgan, *Deterrence Now* (New York: Cambridge University Press, 2003).

[110] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (January 1, 2017): 44–71, https://doi.org/10.1162/ISEC_a_00266; Lindsay and Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited"; Schneider, "Deterrence in and through Cyberspace."

emboldened to use whatever means they have at their disposal to meet their objectives, limited only by efficiency concerns. The challenge lies in between these extremes, where the variable threshold of credibility creates a policy arena for limited conflict, and where it can be difficult to distinguish efficiency motivations from risk sensitivity. Doubling down on deterrence can mitigate conflict in the latter case but provoke escalation in the former.

The same cases that have raised alarms about the dangers of gray zone conflict—Russian incursions in Georgia and Ukraine and cyber campaigns targeting many other countries—also present a convenient opportunity for testing our alternative explanation. The deterrence gradient can be operationalized geographically: credibility is highest for United States immediate deterrence and lowest in Russia's Eurasian backyard, with decreasing values for Western NATO members, newer Eastern members, and European non-members. We found that Russia systematically pulls its punches along this gradient, employing a greater variety of means with more lethal intensity where deterrence is weakest and conducting only ambiguous information operations where deterrence is most robust. Recent Russian interventions offer the paradigmatic exemplars of gray zone conflict, but the conventional wisdom about it is wrong. Russia does not have a general-purpose capability that it can use at will to destabilize any Western democracy or undermine any deterrence posture. Rather it acts opportunistically as circumstances enable it to hassle its adversaries and their clients without, however, risking a military confrontation that it does not desire. The flip side of this logic, however, is that Russia is willing to call NATO's bluffs in cases where it can reasonably expect that NATO is unwilling to intervene. The case of Georgia (and even more so Chechnya and less so Ukraine) illustrates Russian willingness to indulge efficiency considerations (i.e., take the gloves off) when there is little prospect of NATO punishment.

This argument has implications for the debate over NATO expansion after the Cold War. Posed in starkly binary terms, expansion is seen as either a stabilizing force for Europe in the face of Russian recidivism or an irresponsible provocation of legitimate Russian security interests fueled by liberal delusions [111]. If deterrence and conflict are continuous variables, however, then the real question is not simply whether NATO should or should not have expanded its security guarantees, but how far. One might thus argue that the first round of expansion to include the Eastern-Central countries (Poland, Hungary, Czech Republic) under the NATO umbrella helped to stabilize an historically conflict-prone part of Europe in a period in which Russia was willing to accept a downward revision of its European influence after the fall of the Soviet Union. Perhaps later rounds which brought in Baltic and Balkan

[111] Michael McFaul, Stephen Sestanovich, and John J. Mearsheimer, "Faulty Powers: Who Started the Ukraine Crisis?," *Foreign Affairs*, December 2014, http://www.foreignaffairs.com/articles/142260/michael-mcfaul-stephen-sestanovich-john-j-mearsheimer/faulty-powers; John J. Mearsheimer, "Why the Ukraine Crisis Is the West's Fault: The Liberal Delusions That Provoked Putin," *Foreign Affairs*, October 2014, http://www.foreignaffairs.com/articles/141769/john-j-mearsheimer/why-the-ukraine-crisis-is-the-wests-fault.

countries also made sense in whole or part. This is not the place to debate this history. We merely wish to point out that the alternative perspectives of NATO provocation and Russian aggression are better conceived as context specific variables rather than absolute qualities of either actor.

Just as deterrence varies along the gradient, the contours of the gradient can shift over time. When NATO's relative power was increasing, expansion was defensible. If NATO's relative power decreases for whatever reason, then retrenchment makes more sense. Conversely, declining Russian relative power may enable NATO to bolster the line, rendering today's gray zone provocations prohibitively costly tomorrow. As gray zone conflict reveals the contours of the deterrence gradient, especially in areas where the "defender" has overreached its ability or will to respond, actors can take steps to shore up defenses for the things they really value. Russia has advertised its willingness to interfere in elections, distort public debate, mobilize nationalist movements, and engage in other provocations, which in turn has already mobilized a Western response to improve awareness, counterintelligence, defenses, and deterrence postures. Much as the shooting down of the Malaysian Airlines aircraft over Donetsk led both to heightened debate in NATO about the possibility of intervention and to greater restraint on the battlefield on the part of Moscow, so too the lowering of credible escalation thresholds can help to contain risk-averse opportunists. Just as gray zone conflict is symptomatic of deterrence success, the increasing incidence of Russian provocation may be symptomatic of a closing window for its effectiveness, such as it is.

The very fact that an adversary is engaging in limited conflict suggests vulnerabilities and opportunities. Instead of worrying that Russia is outwitting the West, we should instead realize that NATO has already blocked Russia from wielding even more influence. The general deterrence posture of NATO and US deterrence policy has arguably succeeded in keeping the more overt forms of Russian aggression in check. The unfortunate fact remains, however, that a simple remedy for gray zone conflict does not exist and it instead requires constant activity across domains to understand and contain new variations of provocation. Because conflict and deterrence are variable, they must be managed continuously as well.

Appendix