# After Deterrence: Explaining Conflict Short of War[[1]](#footnote-1)

J Andres Gannon1, Erik Gartzke2, and Jon R. Lindsay3

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*

March 2019

## Abstract: Policymakers are increasingly concerned about conflict in the “gray zone,” a region between peace and war where, it is feared, challengers are able to alter the status quo without triggering larger confrontations. A defining characteristic of gray zone conflict is that capable aggressors willingly limit the potency of their attacks. We offer two explanations for this. First, deterrence successes can cause challengers to “pull their punches,” adopting sub-optimal strategies to avoid triggering a larger contest. Defenders in this scenario can respond by “doubling down” on deterrence, further containing the contest and forcing aggressors to choose between withdrawal or continuing to fight inefficiently. Second, challengers instead may deliberately choose the gray zone as a low-cost, militarily optimal, strategy. In this case, doubling down on deterrence is counter-productive and risks escalation. We assess these arguments empirically in Russia’s post-Cold War foreign interventions. We find that Russian gray zone interventions reflect the first motivation (deterrence sensitivity), rather than the second (military optimality). Russian covert cyber and intelligence operations are ubiquitous, while more overt and muscular operations appear inversely with the credibility of Western deterrence, reflecting deterrence success.

Abstract: 184 words

Article: 13,861 words (sans title page)

# Introduction

In the wake of the overthrow of Ukrainian President Yanukovych in February 2014, Russian Spetsnaz (special forces) and the 810th Independent Naval Infantry Brigade occupied the Crimean Peninsula [(Kofman et al. 2017)](https://www.zotero.org/google-docs/?nkanYP). These forces had removed their military insignia, prompting some to speculate about whether or not their actions were sanctioned by the Kremlin. After the dust had settled, most observers took it for granted that Russian forces had conducted an invasion with a deliberate goal of annexing Crimea. As both Russia and NATO were eager to avoid a direct confrontation, the pretense of anonymity was a political fig leaf providing NATO with a convenient excuse to forgo a more forceful response.[[2]](#footnote-2)

Russian occupation of Crimea and subsequent incursions in Eastern Ukraine prompted considerable concern in NATO and elsewhere about how to counter “gray zone conflict,” or actions that fall below agreed upon thresholds for a coordinated military response, but which are clearly destabilizing and inimical to Western interests. On this topic, the British Secretary of State for Defence noted this “[i]s 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” [(Fallon 2017)](https://www.zotero.org/google-docs/?LVsbsP). Many have worried that “little green men” might reappear in the Baltics, conducting incursions without crossing any explicit “red lines” that might trigger a NATO Article V response. Others have described “little blue men” in Chinese efforts to revise the maritime status quo in East Asia [(Erickson and Kennedy 2015; Green et al. 2017)](https://www.zotero.org/google-docs/?lMU7EG). The kaleidoscopic language highlights challenges that are as much definitional as practical. As General Dunford, Chairman of the Joint Chiefs of Staff, recently 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” [(Dunford 2016)](https://www.zotero.org/google-docs/?Ld4t36).

There is, of course, nothing new about conflict that falls ambiguously between peace and war. There is a long history of, and a vast literature on, limited conflict [(Kissinger 1955; Schelling 1957; Osgood 1969; Rosen 1982; Lepgold and Sterling 2000; Sullivan 2007; Powell 2015)](https://www.zotero.org/google-docs/?wedX3q), salami tactics [(Schelling 1966; Fearon 1996; Freedman 2014)](https://www.zotero.org/google-docs/?eirtRm), low intensity conflict [(Freysinger 1991; Grant 1991; Metz 1989; Turbiville 2002)](https://www.zotero.org/google-docs/?8OAVAL), revolutionary war [(Shy and Collier 1986)](https://www.zotero.org/google-docs/?E8cDA8), military operations other than war [(Kinross 2004; Lin-Greenberg 2017)](https://www.zotero.org/google-docs/?L5ADKn), covert operations [(Johnson 1992; Carson 2018; O’Rourke 2018)](https://www.zotero.org/google-docs/?duIGFD), small wars [(Olson 1990)](https://www.zotero.org/google-docs/?wLqJVN), fifth columns [(Charap 2015)](https://www.zotero.org/google-docs/?CitmP9), and proxy wars [(Bar-Siman-Tov 1984; Brown 2016; Driscoll and Maliniak 2016)](https://www.zotero.org/google-docs/?3J7Tya). Many (but not all) of these concepts emphasize asymmetric struggles with at least one combatant that is *unable* in practical terms to fight on a larger scale or with higher intensity. Gray zone conflict, in contrast, features adversaries that 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 Kissinger said, “We need 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” (Johnson 2013). General Votel [(2016)](https://www.zotero.org/google-docs/?N9A0JQ) 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 around the world, resulting in American victory in the absence of a larger overt (nuclear) contest.

The essential puzzle, then, is why capable countries on both sides of the gray zone limit their chances of victory by leaving some of their most potent capabilities — weapons they might normally be expected to wield on the battlefield — at home. Conventional wisdom treats gray zone conflict as a new way of war – rivals are outsmarting the West by utilizing new technologies that allow them to pursue revisionist aims without the West pushing back. We present a second, contrasting logic of deterrence. Challengers may be deterred from engaging in general war by the explicit threats or implicit posture of defenders and their allies, choosing instead to adopt militarily sub-optimal strategies, settling for doing something rather than nothing. In this case, a defender might be able to improve strategic stability by clarifying and intensifying its deterrence posture, in effect making even the challenger’s second-best option look less attractive.

Our discussion of the gray zone proceeds in four parts. We begin by summarizing existing understandings of gray zone conflict, explaining why the phenomena is neither as unique nor alarming as it is often presented. Next we introduce a new explanation for gray zone conflict framed through the lens of deterrence theory that identifies continuity in the ways in which capable actors limit conflict intensity but that differentiates it from other forms of low intensity conflict by emphasizing the motivation of actors. A third step is to conduct a preliminary empirical test of the theory by assessing recent Russian foreign interventions, all of which involve a significant cyber component but which vary in the additional types of tools employed. We find that Russia systematically limits its choice of military means along a gradient of deterrence credibility, increasing from East to West. This can be explained if the actual manifestation of Russian aggression is in fact a “second best” reaction to the success of Western deterrence, rather than newly potent or merely efficient means of Russian influence. Finally, we conclude by highlighting key implications of our argument.

# Between Peace and War

Contemporary security policy discourse in the United States, and in the West in general, is characterized by pessimism about a new and poorly understood way of war, referred to by many labels, but often called gray zone conflict. The United States Special Operations Command (SOCOM) defines gray zone conflict as [(Bragg 2017)](https://www.zotero.org/google-docs/?D0eHwM):

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.

Amidst evolving definitions, a recurring dilemma for policy makers has not been *whether* to respond to gray zone aggression, but *how*. In the last decade of the Cold War, Secretary of State Schultz argued that the United States needed a strategy to counter ambiguous warfare that made it unambiguous America would fight back [(Schultz 1986)](https://www.zotero.org/google-docs/?dsk0uW). Contemporary US policy makers have similarly decided that whether new or renewed, gray zone aggression requires a strategic response characterized by countering misinformation [(Paul and Matthews 2016)](https://www.zotero.org/google-docs/?StaQYN), adapting to risk sensitivity [(Maxwell 2016)](https://www.zotero.org/google-docs/?Pwx0YG), and responding with non-military means where gray zone conflict resists military solutions [(Galeotti 2016)](https://www.zotero.org/google-docs/?8TQfwe).

## Historical Conceptions of Limited War

While it is conventional (and convenient) to think of peace and war as dichotomous, discrete outcomes, observers have long recognized that tension and violence exist on a spectrum [(Lebow 2010)](https://www.zotero.org/google-docs/?vbdeyO), even as the relevant descriptive language evolves. 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 war in the shadow of nuclear weapons (war limited by costs - i.e., deterrence), and low-intensity conflict with irregular forces (war limited by means). After the Cold War, only the last of these received consistent attention, especially after the United States found itself engaged in Afghanistan and Iraq and practitioners began to dust off old texts looking for lessons about counterinsurgency. The novelty of gray zone conflict today, involving capable near-peer competitors exploiting new intelligence capabilities, in many ways represents a return to the two preceding themes. Indeed, one of the key insights that inhabits these earlier literatures, but which to our knowledge was never made explicit, involves the need to distinguish between types of limited war in order to apply appropriate policies.

### Wars Limited by Ends

In a government memorandum, George Kennan [(1948)](https://www.zotero.org/google-docs/?QI5R2R) discussed limited war between peer competitors when he emphasized that both overt and covert political warfare could play a role in Western 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.

The emphasis on limited political objectives over military operations represented the key shift in thinking about limited war. 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 (Osgood 1969; Wagner 2000). Even at this time, limited war was understood as occurring when actors had the capacity to increase their commitment but did not want to do so, creating a third option short of major war and beyond acquiescence (Kissinger 1955; Brodie 1957; Kissinger 1957). Kissinger and Osgood tried to figure out ways to conduct limited war and avoid escalation by restricting targets and weapons systems as well as applying techniques to limit the geographic scope of conflict (Woodman 1991). Clearly, there are difficulties in maintaining this third option. Mutual recognition of the limits to conflict must be common conjecture among adversaries (Schelling 1957). During the Vietnam war, the North Vietnamese leadership was prepared to escalate conflict despite efforts by China and the Soviet Union to restrain their ally (Carver 1986).

### Wars Limited by Costs -- Deterrence Contests

Cold War strategists advanced the notion of “the stability-instability paradox” (Snyder 1965; Jervis 1984) to explain how incentives for engaging in conflict at lower levels of intensity or in peripheral theaters arise out of disincentives for initiating major nuclear war (or even major conventional war). According to Snyder (1965), “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.” While there are strategic benefits that come from “weakening the enemy with pricks instead of blows” (Hart 1954), there are also risks to this approach in the nuclear era. The presence of nuclear weapons might prevent world war, but it could simultaneously encourage localized aggression or smaller, more limited conflicts (Russell 2003; Sagan and Waltz 2003; Kapur 2007). Modern empirical elaborations of stability-instability analyze the situation quantitatively (Rauchhaus 2009; Early and Asal 2018) or in specific contexts, like India and Pakistan (Ganguly 1995; Raghavan 2001). Yet recent studies criticize stability-instability because the theory and practice are out of sync, pointing to the need for updated conceptions of deterrence (Powell 2015; Schram 2019).

### Wars Limited by Means

## The primary examples of the stability-instability paradox during the Cold War were decolonization struggles and proxy wars in the Third World. Limited war with irregular forces as opposed to near-peer competitors garnered much attention in the 1970s under the rubric of “low intensity conflict” or LIC (Schultz 1986). Opinions differ as to what distinguishes LIC from conventional war. Some approaches focus on means (Kornbluh and Hackel 1986; Adams 1990) while others identify the phenomenon by actor (Downie 1992; Kinross 2004). One commonality is a focus on strategies of the weak. Unsurprisingly LIC is more prevalent in poor and poorly institutionalized regions (Kornbluh and Hackel 1986; Hammond 1990; Kober 2002). The classical literature on counterinsurgency (Galula 1964; Taber 1965; Thompson 1966; Kitson 1971; Blaufarb 1977) and its modern revivals (Nagl 2005; US Army 2006; Ucko 2009; Kilcullen 2010) largely fall into this category. A vast academic literature on civil war examines the behavior, motives and organizational structure of “non-state” actors (Petersen 2001; Wood 2003; Kalyvas 2008; Shapiro 2013).

## A Silver Lining to Modern Gray Zone Conflict

Modern gray zone conflict is in many ways a return to the familiar stability-instability paradox, though often with different, usually lower, thresholds. Deterrence now results as much from the risk of escalation to major conventional war, or even economic disruption, as by the threat of nuclear conflagration. The real novelty, however, is in the growing diversity of ways in which low intensity conflict can be practiced. At the same time that the *whom* of conflict has reverted to more familiar state actors, the *how* has evolved subtly. The emergence of new, cheaper implements of coercion associated principally with information technology have made it easier to fight circumspect contests.

Russian activities have been described as emblematic of this logic. Ukraine demonstrates a strategy of hybrid warfare that occurs when the belligerent has escalation dominance and revisionist aims [(Lanoszka 2016; Marten 2015; Thomas 2015)](https://www.zotero.org/google-docs/?J3Wqyh). Outside of the Ukranian context, broader concerns about Russian gray zone activities paint a dismal picture, arguing that Russia’s declining military power and new, cheaper forms of warfare will sponsor increased aggression against NATO and the West [(Charap 2015)](https://www.zotero.org/google-docs/?xVr9A5). This view holds that states can deploy gray zone tactics strategically to work around their adversaries’ red lines to achieve coercive bargaining success without triggering escalation [(Altman 2017; Jackson 2017; Lin-Greenberg 2017)](https://www.zotero.org/google-docs/?sSwMVt). What one should thus observe is 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 demonstrates an actor’s escalation dominance. Even when analysts recognize that lower intensity conflict is not novel, they tend to highlight the expanded repertoire of military strategies available, especially emphasizing online subversion and cyber disruption [(Jensen, Valeriano, and Maness 2019)](https://www.zotero.org/google-docs/?QrBwwF). Yet the apparent expansion of means cannot in itself imply a restriction of practice. Accounting for this circumspection is then the central logical challenge in understanding gray zone conflict. Why don’t capable countries use all of their capabilities, maximizing their prospects for victory, at least in narrow military terms?

That gray zone conflict could be worse is perhaps a modest silver lining. A note of cautious optimism in this regard was expressed by the Secretary of State Shultz:

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” (Schultz 1986).

In sum, the emergence of gray zone conflict can be understood as a symptom of strength rather than a product of weakness. Our theory focuses on this dynamic, emphasizing and explaining this good news (restraint) about the bad news (conflict).

# A Theory of Gray Zone Conflict

## A Typology of Limited 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 empirical reality of an overlap with other concepts, such as low intensity conflict and limited war, while at the same time emphasizing unique attributes of conflict in the gray zone. While limited war is not a new phenomenon, gray zone conflict does differ from prior conceptualizations of limited war that focus on conflicts in which actors are limited by their means or costs because the motivation for gray zone conflict can vary.

Our definition highlights three important aspects of conflict in the gray zone. First, gray zone conflict results from agency rather than necessity. It is *limitation by choice*. Earlier concepts of limited war that focused on limited ends ignored the full portfolio of means available to an actor for war. Recommendations for “whole-of-government” approaches that combine multiple political and military capabilities to compensate for conventional military weakness (Chivvis 2017) fail to distinguish gray zone conflict from other forms of conflict that also utilize non-military means (political, economic, informational, humanitarian). It is important not to conflate the increasing variety of tools available for conflicts of all types with the use of *some* of those tools for gray zone conflict. One must first understand the general logic: gray zone conflict involves “pulling punches” where more of a state’s portfolio of coercive tools are left unexercised.

Second, gray zone conflict involves *capable initiators*. This differentiates activities that Russia or the United States undertake from actions taken by insurgent groups, for instance, even in cases where operations appear similar. Table 1 distinguishes the motivations and constraints that lead actors to engage in different types of limited operations. Less capable actors can pursue limited war, while sustaining their efforts with oversized expectations (i.e., revolution). But actors that have a lot can either try to get their way by force (traditional conflict) or just marginally shift the balance of power (gray zone).

**Table 1**: Actor’s Conflict Typology

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **Ends** |
|  |  | Concessions | Conquest |
| **Means** | Smaller and less diverse forces  Larger and more diverse forces | Limited War  Gray Zone | Revolutionary War    Traditional Conflict |

Third, gray zone conflict must be *mutually preferred* by both sides in a contest. By its nature either side in a gray zone conflict can escalate, but neither side chooses to do so. Although consistent with the assumptions behind theories of wars limited by cost (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 own reaction to the provocation. Anticipating this, the attacker selects technologies that deliberately obfuscate its intentions or complicates attribution. This is done more 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. Covert conflict is a form of collusion between adversaries to avoid mutually harmful escalation (Carson 2015; Carson 2018). Cases like Russia’s “little green men” in Crimea can also be understood as efforts to work around opponents’ red lines by “advancing without attacking” in order to achieve objectives without resorting to major war (Altman 2017).

## Two Logics for Gray Zone Conflict

An actor undertakes gray zone conflict when the expected benefits of doing so exceed the expected payoffs from ordinary competition and traditional conflict. This gives rise to two possible preference orderings:

Gray zone ≿Ordinary competition ≿High intensity conflict

Gray zone ≿High intensity conflict ≿Ordinary competition

The first describes gray zone conflict motivated by *deterrence*. Military retaliation or other related consequences (sanctions, etc.) resulting from the overt use of force are deemed sufficiently costly that the initiator refrains from pursuing it. The second reflects gray zone conflict motivated by *efficiency*. The attacker is willing to go to war to achieve its objective, but gray zone conflict is an easier way to achieve them at lower cost. Conventional wisdom has focused on the latter – efficiency – rather than differentiating these two contrasting logics. The key difference is how the attacker is likely to respond if operating in the gray zone becomes more difficult as a result of increasing coercive pressure from the target or others. The first type of actor should back down, preferring peace to war, while the second will escalate in response, preferring war to peace.

### Gray Zone Conflict as a Product of Deterrence

Contrary to alarmist perspectives, much of gray zone conflict actually reflects deterrence success. Initiators in the gray zone are choosing to initiate contests with limited means in part because they are intimidated by the risks/consequences of escalation by a target or its partners. Initiators in these circumstances are not choosing to fight as they most prefer but instead choose militarily sub-optimal modes of conflict for political reasons. They are deterred. As a result, the initiator cannot expect to perform especially well on the battlefield, as its fear of escalation prevents implementation of a more effective strategy.

Ukraine is a commonly misunderstood example. Here, NATO has conventional escalation dominance, should it decide to intervene on behalf of Ukraine for some reason. Russia would most likely lose a conventional contest involving NATO, risking escalation to nuclear war in the process. The risk of triggering a robust NATO reaction appears to have led to considerable 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 (Smith-Spark and Master 2018). The presence of gray zone conflict in Ukraine is thus emblematic of a significant deterrent effect on Russia’s operational efforts, despite the fact that NATO has no formal commitment to Ukraine.[[3]](#footnote-3)

The gray zone thus functions as a policy arena formed by and below thresholds created by deterrence (formally or practically, explicitly or implicitly). While not new per se, gray zone operations also become 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 through interdependence and coordinate 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.

Schelling (1966) 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.” Gray zone poses a different relationship in which a capable actor may choose to engage in limited war precisely to *lower* the risk of larger war (Schram 2019). 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 defender can generate” (Powell 2015). Mutually constrained actors pursue (and resist) aggression furtively, so as to protect broader cooperative or compatible goals.

A key implication of this perspective is that, for actors in this category, raising the costs or risks of gray zone conflict can further inhibit or even prevent them from acting more aggressively. 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 intensifying the chicken dynamic of deterrence, or lowering conflict escalation thresholds, can help to contain conflict in the gray zone. In a world where gray zone strategy has been chosen because of a fear of escalation, tying aggression in the gray zone to a retaliatory response should force an initiator to think twice. This “doubling down” on deterrence begs several questions about the motivation and resources, but technically it does follow from our logic.

### Gray Zone Conflict as a Product of Strategic or Tactical Efficacy

If the first explanation for gray zone conflict involves inherent tensions between the use of force and its consequences, the second argument requires no such contrast. Initiators (and their targets) may have decided that pulling their punches is, in fact, optimal. A challenger that is patient and capable relative to its adversaries at low intensities might benefit by choosing a gray zone strategy. Current attention to gray zone conflict focused almost exclusively on this dimension. While high intensity conflict may 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 (Altman 2017).

The efficiency scenario carries the opposite policy implication from the deterrence case. If the initiator chooses gray zone conflict because it is a lower-cost means to achieving its goals, then raising costs in the gray zone reduces the attractiveness of limited means strategies to the initiator, thus encouraging it to escalate. Escalation may, in fact, be desirable for the target. Assuming that gray zone conflict is not optimal for the target, the target can exploit the escalation effect of inefficient warfare by raising the cost of gray zone conflict, thus preventing the initiator from exploiting a low cost means of achieving its goals. In essence, by raising the cost of gray zone conflict, the target can force the initiator into fighting less efficiently, *but only by also accepting higher costs/risks themselves, something that may be mutually unappealing*.

## The Role of Third Parties

As the logic above is dyadic, the role of third parties deserves comment. Many treatments of covert warfare focus on military aid to local proxies from a powerful patron. Lanoszka (2016) emphasizes that the 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. This would preclude our deterrence story, but deterrence again becomes an important shaping influence when we take into account asymmetric resolve or the effect of alliances between the weaker state and more powerful protectors. Russia may not be deterred by the Ukrainian military, but it must take into account the risk of triggering an unwanted NATO in calibrating its actions. A more complex portfolio of actors can thus be boiled down for analytical purposes (at least initially) to our dyadic conception of gray zone conflict; for convenience, a target’s allies or friends can be considered as part of the target’s capabilities, and the level of commitment in an alliance can be factored in in terms of the overall strength of deterrence.

Thinking of allies or other partners as a component of the initiator or target’s power, discounted by the probability of third-party intervention, suggests that more actors are “capable” than when considered in purely bilateral terms. Importantly, alliances and other attempts to aggregate capabilities are often explicitly or implicitly designed to generate deterrence by reducing agency (autonomy) on the part of individual nation states, making them behave more like a single unit—not unlike our assumption (Sobek and Clare 2013). Deterrence works if an ally might respond to a given provocation, but gray zone conflict occurs nonetheless precisely because an ally might not intervene. Indeed, the existence of interested third-parties can transform cases that would have been limited war into gray zone conflicts. Interestingly, the explicit delineation of a deterrence *quid pro quo* probably increases this risk, as red lines clarify what can be achieved in the gray zone.

In sum, capable actors pulling punches (alone or through proxies) is not explained simply by limited ends or by fear of escalation, but by both processes operating interactively. States in the modern world still disagree enough to take steps to alter the distribution of power and benefits, despite desiring peace and wishing to limit the costs of conventional conflict. Gray zone conflict may also simply be more efficient. The presence of contrasting motives explains why in some cases, increasing the cost of gray zone conflict can lead an initiator to de-escalate in favor of ordinary competition (gray zone motivated by deterrence), while in other instances it encourages an initiator to escalate (gray zone motivated by efficiency). We argue that it is the deterrence explanation that has become more common in the 21st century.

# Russian Gray Zone Campaigns

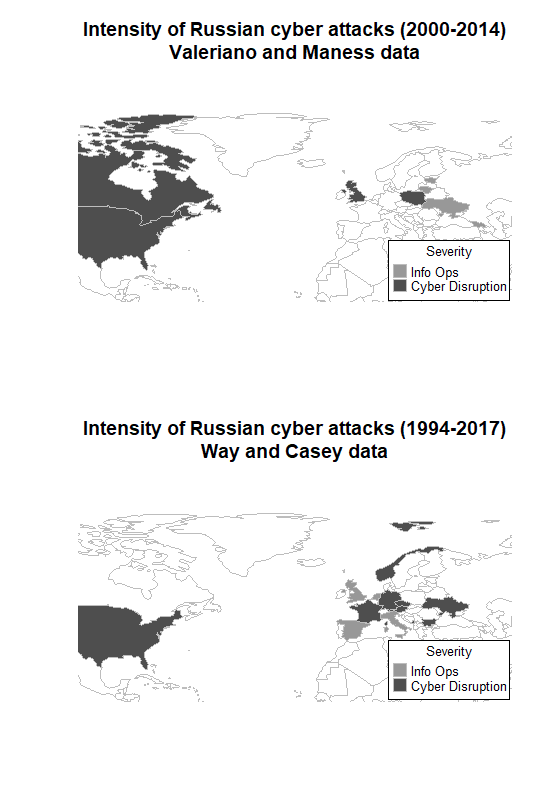
In this section we test the plausibility of our argument about deterrence sensitivity by examining major Russian foreign interventions over the past two decades. Most cases feature cyber campaigns for disruption or influence, and some also feature intervention by special operations or conventional forces. 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 (Freedman 2014; Marten 2015; Driscoll and Maliniak 2016; Lanoszka 2016; Chivvis 2017). Along the way we introduce the notion of a geographical deterrence gradient, modeled on the military loss-of-strength gradient (Boulding 1962), as an instrumental variable to proxy for various factors that can affect the strength of deterrence. We then review four major Russian cyber campaigns that have targeted states differentially located on this 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 circumstances of deterrence.

## 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. The two cross-national datasets (Dyadic Cyber Incident and Dispute V1.1 (DCID) by [Valeriano and Maness (2014](https://www.zotero.org/google-docs/?FHYpOD))) and Russian Electoral Interventions (REI) by [Casey and Way (2017](https://www.zotero.org/google-docs/?6Y9Yic))) cover almost entirely distinct samples. The severity of Russian cyber operations also reveals major coding heterogeneity.[[4]](#footnote-4)

Figure 1 shows the severity of Russian cyber operations coded by the two cross-national datasets. Each paints a distinct picture of the primary targets of the most severe Russian attacks.[[5]](#footnote-5) The 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. Part of this discrepancy is due to the respective foci of each dataset; DCID seeks out cases of cyber incidents and disputes while REI focuses on Russian electoral interference. While a majority of the REI cases include some form of Russian cyber activity, there are a few cases where only material support was provided (eg. Moldova 2014 and Belarus 1994). This discrepancy exemplifies not only the challenges of relying on open source reporting for identifying cyber influence or disruption campaigns, but also differences in defining what counts as an attack.

**Figure 1**: Prior Analysis of Russian Cyber-attacks



These two datasets give 71 unique cases of Russian aggression that either included some degree of cyber intervention or were cases of electoral interference. Using the combination of these two datasets as a starting point, we add 10 new instances of Russian cyber-attackcyber-attacks from 1994-2018 and also include 3 cases of non-cyber Russian aggression during this time period from the International Crisis Behavior dataset [(Singer, Bremer, and Stuckey 1972)](https://www.zotero.org/google-docs/?x6hYqQ).[[6]](#footnote-6) This has the further advantage of not focusing exclusively on Russian cyber-attacks but also including all Russian conflict short of war. The unit of analysis is the country-year, with 82 cases of Russian intervention from 1994-2018. Second, we code new variables concerning variation in how Russia conducted its attack. In some cases, cyber-attacks were limited to information operations. In other cases, Russian actions included more severe actions, such as DDoS attacks and attacks on critical infrastructure, or even uses of force by paramilitary or conventional military units.[[7]](#footnote-7) Some cyber-attacks may result in disruptions that are temporary or easy to mitigate (DDoS). Others may be more permanent and physically destructive (industrial control system sabotage). Cyber exploitation (espionage) falls somewhat in between the two levels of cyber aggression as attackers may use software hacking techniques but try to avoid detection by not disrupting normal user operations.

For each incident, we code whether Russia used conventional ground forces, conventional air or sea forces, paramilitary or covert forces, cyber disruption, and information operations. By distinguishing between these five types of aggression, we obtain a clearer picture of the intensity of each case of Russian intervention. The vast majority of cases include at least some type of cyber operations. In a few cases, data limitations preclude coding of non-kinetic activity by Russia or other actors. In Moldova 2005, for example, Russia provided material support for the Communist Party but there is no credible evidence of cyber activities.

Figure 2 describes our analysis 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). We posit that the recent concerns about Russian gray zone operations is driven not by an increase in their intensity, but by the higher frequency of their occurrence.

**Figure 2**: Intensity of Russian intervention over time

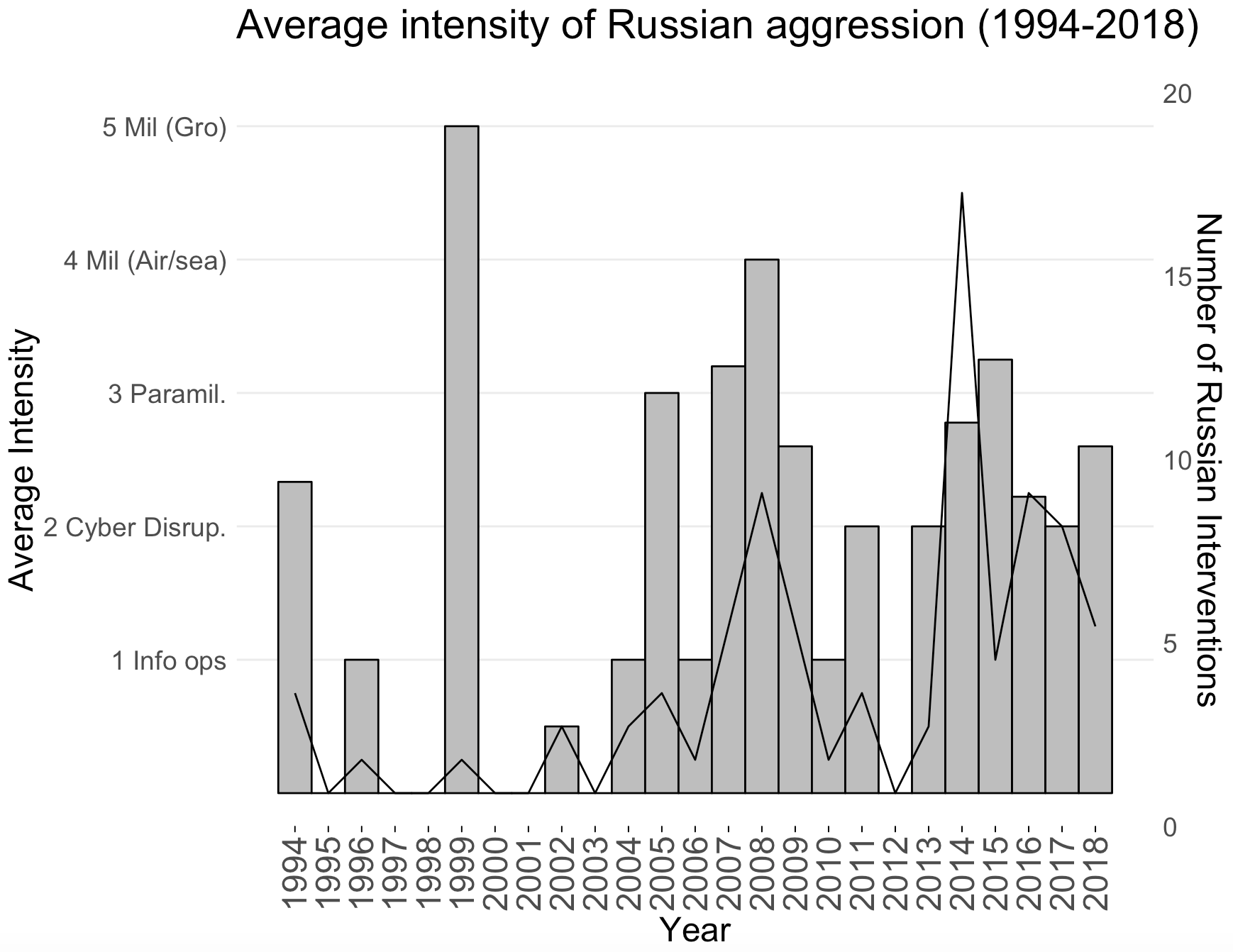


Figure 3 depicts the relationship between geography and the intensity of Russian operations. To prepare the figure, we compiled an entirely new coding of the intensity of Russian attacks, independent of codings in previous datasets. Here, DCID and REI are used primarily for initial case selection. The previous heterogeneity in coding has thus been resolved. Russia seems less likely to engage in kinetic escalation if the conflict zone is further from its border. Inversely, Russia is more likely to escalate in nearby territories. While Russian influence operations are pervasive, cyber disruption is less common, and intervention with military force occurs only in Russia’s immediate periphery (its “near abroad”). The exception to this geographical pattern is in Syria, site of a major Russian naval base on the Mediterranean.

**Figure 3**: Geographic representation of Russian intervention



## The Deterrence Gradient

To explain the geographical pattern of Russian gray zone operations, we posit a deterrence analogue to the military loss of strength gradient (Boulding 1962).[[8]](#footnote-8) 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 rather that it is a useful proxy for other factors that do (capabilities, interest).

Insofar as military power is affected by a loss of strength gradient, deterrence at distance should be less robust than proximate deterrence. There are also reasons to expect resolve to vary with distance. All things being equal, states likely care more about issues nearby than those that are far from home. Defenders are thus more resolved to resist aggression on their borders, even as distant attackers are less capable or resolved. Alliances to nearby states should similarly be more credible since patrons are more willing to defend a proximate client (Bak 2018). Alliance commitments should be less credible with distance as well, as patrons will fear entrapment by distant, more highly resolved allies (i.e., chain-ganging).

A fundamental question about nuclear deterrence during the Cold War was *not* whether the United States was *able* to inflict terrible punishment on the Soviet Union—nuclear weapons made this obvious—but whether it was *willing* to do so. While the United States could be expected to retaliate for nuclear attacks on its own soil, many questioned its willingness to trade Washington for London or Paris. Extended deterrence—the use of threats to protect allies beyond a state’s borders—is widely believed to be less credible than homeland deterrence (Fuhrmann 2018). The Cold War solution to this problem was the forward deployment of American troops in Europe as a visible commitment mechanism. This practice continues today on a lesser scale with tripwire forces currently deployed in the Baltic states.

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. The Russian port of Tartus is important in both regards as a staging base for Russian combat operations in Syria and may help to explain the Syrian exception to the East-West pattern in the intensity of Russian operations in Figure 3. Just as not all outposts are created equal, furthermore, some commitments are stronger than others. While NATO security guarantees nominally cover all 29 members equally, the 12 founding members in Western Europe and North America are arguably more confident in this commitment (George and Sandler 2018). Indeed, recent Eastern European entrants have questioned NATO resolve. Declarations from NATO leadership that there are no second tier members simply underscores this concern. Eastern European NATO members also appear to have greater need of the NATO insurance policy given that Russia is both more interested in, and more able to, control territory on or near their borders (Noetzel and Schreer 2009; Matláry 2014). In sum, Western resolve/capability decreases from West to East while Russian resolve/capability increases.

Wither cyberspace? 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 (Goldsmith and Wu 2006). The geographical metaphor of “cyberspace” ignores overlapping institutions and infrastructures that enable states to share information (Branch 2018). If global information systems have some characteristics of a commons it is because interconnection is in the interest of the stakeholders who make and maintain them (Drezner 2004; Raymond 2013; Sowell 2015). What happens in the cyber domain is conditioned by what happens in other domains. We thus expect the interaction of a global domain with more localized domains to impose geographical constraints on the distribution of conflict in that domain.

A naval analogy is helpful. Corbett (1911) argues that navies are better suited for limited war than armies because the ocean provides access to distant resources that an adversary is less resolved to defend. A state is less likely to make the effort to recover a colony detached and defended by an enemy fleet than to resist a threatened invasion of its homeland. When the stakes increase, naval power is typically combined with expeditionary or allied land forces. Applying Corbett’s logic, expanded digital reach might be similarly useful for limited aims operations that do not directly threaten vital interests. Indeed, ubiquitous computers enable intelligence, influence, and counterintelligence at a grand scale. Yet while online abuse is troublesome and can be costly, it seldom provokes a military response. Disruption or destruction of physical infrastructure, moreover, happens very infrequently compared to the epidemic of espionage and abuse online. To date, tbe striking empirical trend in cyber conflict restraint (Valeriano and Maness 2015). High-end cyber conflict could be more attractive in conjunction with war in other domains, but that sort of war itself is a rare event.

The cybersecurity literature offers two logics for the muted nature of cyber aggression. Geography plays a tacit role in both. First, the complexities of planning and conducting offensive cyber operations against sensitive targets and the possibility of active defense create a sort of deterrence by denial (Lindsay 2013; Gartzke and Lindsay 2015; Buchanan 2016; Slayton 2017). Distance matters because the remote intelligence needed to plan and monitor offensive cyber operations, which often include human intelligence, are harder to obtain. Second, the likelihood of attribution and the possibility of retaliation in different domains create a sort of deterrence by punishment (Gartzke 2013; Lindsay 2015; Borghard and Lonergan 2017; Schneider 2019). Distance matters in this case because the ability and will to use capabilities in other domains is constrained by distance. We should expect actors to employ destructive cyber operations only in situations where they are confident in their abilities and expect the target to be disinclined to escalate. It is notable that the Stuxnet operation involved a local partner in Israel and American escalation dominance over Iran.

Figure 3 is consistent with a geographical interpretation of deterrence. 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. 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.

## Significant Cyber Campaigns

Russia is involved in numerous gray zone conflicts, but the actual shade of gray in each case depends on the deterrence gradient discussed above. 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. Cyber operations are particularly attractive in strategically constrained situations, as argued above, so it is instructive to examine the broader cross-domain context and response in each 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 (Driscoll and Maliniak 2016; Götz 2017). We do not focus here on the origins (micro-foundations) 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. Rather we argue that how motives are expressed, whatever their origins, will be more or less constrained by the prevalence/intensity of deterrence.

We thus expect that the deterrence gradient conditions Russian intervention in each case. We employ a most similar case comparison (Bennett and Elman 2007) 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. 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.

**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 their distance from Washington DC.[[9]](#footnote-9) 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 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. Russia intervened in Georgia using overt military force, as well as cyber-attacks.

### 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” (Davis 2007) 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.[[10]](#footnote-10) 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 (Traynor 2007). The attacks continued in some 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 (Schmidt 2013).

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 not yet been clarified (Joubert 2012), which provided both an opportunity and a constraint for Russia. 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 (Carson 2018).

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 (Deibert et al 2012). 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 Georgian civil war after the Soviet collapse, Russia had 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 (Driscoll and Maliniak 2016). 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 a peace agreement on 15 August which left Russian forces stationed in the de facto autonomous provinces (Shakarian 2011; Brecher et al 2017).

Russia’s intervention choices in this conflict were motivated by efficiency, not 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 (2016) 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.” 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)

An alternative explanation for the pattern in Table 2 is that Russia values the stakes differently in each conflict and thus the correlation with the deterrence gradient is spurious. The cases of Estonia and Georgia appear to be consistent with this alternative. 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. On the basis of different Russian priorities, one might try to explain the single-domain response to Estonia versus the multi-domain engagement in Georgia in terms of efficiency alone. The case of Ukraine, however, puts this alternative to the test and finds it 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 salient. As Driscoll and Maliniak (2016) point out, Russian military planners express significantly more concern over NATO forward deployment in Ukraine than in Georgia.

The Western deterrent response in the wake of the Maidan crisis was accordingly muted, consisting mainly of economic sanctions, deployments of U.S. fighter jets to Poland, and eventually arms and assistance to Kiev, but no NATO ground forces on Ukrainian soil. Fighter jets would, of course, be ideal for attacking Russian armored columns in a conventional war, but their very mobility makes them a weak signal of commitment compared to a counterfactual ground force deployment (Gartzke and Kagotani 2017). 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.

Yet while the Western deterrence posture was weak in Ukraine, it was also not nothing. If Russian moves were motivated by efficiency rather than deterrence, then we would expect to see a more overt Russian military response (at least similar to Georgia, which is valued even less than Ukraine). On the contrary, Russia has taken 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.

An actor that pulls its punches can indeed create high costs in an absolute sense. 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 (Driscoll and Steinert-Threlkeld 2019). Covert interventions, even open secrets like Moscow’s deployments to Ukraine and aggressive cyber operations, can convey both resolve and restraint (Carson 2018). 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 (2017) rightly point out, the Ukraine conflict differed in displaying a breadth of conflict modes but without sufficient intensity to warrant outside intervention.

### United States (2016)

The most recent of the four major Russian cyber campaigns is both the most restrained and potentially most consequential. By now, there is 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 Facebook, and infiltrating lobbyist groups (Marten 2017; Rovner et al 2017; Jensen et al 2019). President Obama was aware of the Russian campaign in summer 2016 but did not publicly reveal his knowledge for fear of influencing the election (Fidler 2016). A joint U.S. intelligence community statement (Office of the Director of National Intelligence 2017) 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.”

It is unclear whether the Russian influence campaign had a marginal effect on voters in what was, by any account, a singularly unique and chaotic election. 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 (Sides et al 2018). 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. The investigation by Special Counsel Robert S. Mueller III into “coordination between the Russian government and individuals associated with the campaign of President Donald Trump” (Office of the Deputy Attorney General 2017) is still ongoing as of this writing. Yet after a series of high profile indictments, the question is no longer whether there was collusion with the Russian government but how much and, further, how was candidate Trump involved. If Trump’s victory or subsequent policies as President of the United States can be credited to active measures by the Russian Federation, even in part, it would amount to perhaps the most consequential intelligence campaign in history.

Within the scope of a covert election influence campaign, Russia pulled out all the stops. Moscow orchestrated a diverse suite of operations ranging from technical computer network exploitation and media influence operations to human intelligence (DiResta et al 2018; Howard et al 2018). Its full-court press could be described as unrestrained, even brazen, and thus motivated 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 it do? As a matter of general deterrence, it could be safely assumed that United States was resolved to defend itself from armed attacks directly against it.[[11]](#footnote-11) Overt military attacks certainly, but destructive attacks of any kind, would in all likelihood invite retaliation from the most powerful military in the world. 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. As it stands, Russia's electoral interference has gone essentially unpunished by the United States, aside from the expulsion of some Russian intelligence officers and the application of additional sanctions.

## Discussion

The Russian pattern of intervention acts is largely consistent with the claim that deterrence encourages powerful states to pull their punches. As the deterrence gradient drops off from West to East, however, Russia is more able to indulge in efficiency calculations when deciding how to achieve its international objectives. This correlation would not be present if conflict intensity were limited only by factors like the means available or calculations about the most efficient way to conduct operations. While Russian interests vary, Ukraine reveals that Russia is sensitive to deterrence even when its interests are high. While strategically more important, Russian actions in Ukraine are 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 incentives rather than technological capability. Gray zone conflict is not so much about the utilization of an expanding toolkit as a calculated decision about what should be drawn from that toolkit.

# New Shades of Gray

Conventional wisdom imagines a strong, innovative provocateur outsmarting status quo actors by acting in many domains. By contrast, we see a return to familiar forms of covert conflict short of war waged by powerful peers, albeit with some novel (digital) means. Cyberspace poses many strategic and operational difficulties, to be sure, and observers are right to note the innovativeness, diversity, and relentlessness of cyber operations in contemporary cases. Yet the essence of gray zone conflict--a reduction of possible means for the pursuit limited ends--should not be conflated with the utilization of new capabilities. Cyber warfare may be prevalent in gray zone conflicts, but it will be prevalent in every war of the 21st century.

The key implication of our argument is that gray zone operations are a consequence of deterrence success. If deterrence is to keep up with these challenges, it must continue to adapt as well. In a sense, deterrence is ultimately a strategy to buy time against an adversary committed to changing the status quo. George and Smoke (1989) raise the issue of “designing around” deterrence as adversaries consider options that “offers an opportunity for gain while minimizing the risk of an unwanted response by the defender” (George and Smoke 1974, 1989). Sometimes this can result in serious fighting as when Egypt “designed around” Israel’s deterrent in 1973 (Stein 1989). Even so, “designing around” deterrence is a perverse symptom of its success if the adversary limits its means and aims, even in cases where the target panics and fears that the attacker’s aims are not limited (as Israel did). Others share this perspective. Lieberman (2012) argues that “designing around” is a sign of successful deterrence because an adversary has shaped its challenge in response to the anticipated reaction of the defender.

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 (threats issued in a crisis situation); modern gray zone conflict may more often works to compromise *general* deterrence (implicit barriers to crisis initiation). 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. General increases in the costs of traditional conflict--the carrot of economic interdependence and stick of conventional retaliation--create incentives for the subversion rather than the transgression of general deterrence. The cyber domain, where general deterrence is unreliable and immediate deterrence works hardly at all (Lindsay and Gartzke 2018; Schneider 2019), is well suited to such purposes.

The two different logics of gray zone conflict--deterrence and efficiency--make contrasting predictions. An actor wishing to change the balance of power can do so through ordinary (peaceful) competition, gray zone conflict, or traditional conflict (Schram 2019). Each strategy differs in terms of its ability to alter the balance of power as well as its costs. Efforts to deter gray zone conflict can thus be stabilizing or escalatory, depending on the preference ordering of the initiator. Raising the cost of gray zone conflict when it is motivated by deterrence discourages escalation since the threat of retaliation invokes the very costs that the initiator is hoping to avoid. When motivated by efficiency concerns, however, the initiator has already decided that the expected gains from traditional conflict exceed the benefits of peaceful competition. Thus, raising the cost of gray zone conflict simply makes the gray zone less efficient, encouraging a move to high intensity conflict. Political ends rather than technological means determine the potential for escalation. The problem of escalation in limited conflicts with unlimited potential for violence remains one of the most pressing open strategic problems of the 21st century.

The pessimistic view of the gray zone puts the cart before the horse; “conflict short of war” is neither a new phenomenon nor a cause for alarm. Gray zone conflict 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 (Mazarr 2015). This pessimism has even led some to advocate revamping deterrence to focus on threats from the gray zone (Santoro and Blosserman 2016; Foust 2016; Jackson 2016). But rather than being the efficient utilization of new technologies that leave the target without adequate defense, gray zone conflict should instead be interpreted as a capable aggressor’s unwillingness to escalate a conflict in situations where they possess the ability to do so. Before jumping to the conclusion that gray zone conflict against the United States reflects a failure of deterrence, policymakers should pay attention to why a challenger has chosen gray zone conflict in the first place. The very fact that an adversary is engaging in limited conflict suggests vulnerabilities and opportunities. An empirical examination of recent Russian cyber operations demonstrates the utility of identifying the logic behind strategically holding back; Russia has limited the intensity of its intervention in cases where Western deterrence is most salient. NATO and US deterrence policy has arguably succeeded in keeping the more overt forms of Russian aggression in check. Given this, the West can effectively deal with Russian gray zone operations by recognizing the situations where its deterrence threat is credible and those where a NATO reaction is instead interpreted as an unrealistic overreach. In cases of the former, the West can communicate to Russia that these incursions warrant a retaliatory response that Russia is likely to find prohibitively costly. Concerns about NATO provoking Russia misinterpret Russia’s actions – gray zone activity signals that Russia has flinched in light of Western deterrence. Instead of being concerned that Russia is outwitting the West, NATO states should instead realize they have blocked Russia from yielding more influence because of its assertiveness. Although this paper primarily discussed the Russian context, Chinese activity in the South China Sea should be interpreted in a similar light. The decision to advance via “little blue men” as opposed to more overt military options is a strategic decision that requires rethinking the efficacy of Western deterrence [(Erickson and Kennedy 2015; Gady 2015)](https://www.zotero.org/google-docs/?LlG1Tp).

Whether Western reactions to Russian gray zone provocations escalate or de-escalate is a function of the degree to which credible Western deterrence motivated such limited provocations in the first place. As the geographic scope of conflict moves West, we should expect the United States to be better able to deter further Russian escalation by conveying its dissatisfaction with Russian aggression. US grand strategy must therefore toe a difficult line; trying to understand the motivation for gray zone conflict and reacting accordingly. The classic debate in security studies between the deterrence model and the spiral model applies to gray zone conflict in a novel way. The unfortunate fact remains 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 (Colby 2018). While traditional understandings of the deterrence and spiral model of conflict posit the status quo actor as the determining actor, we instead find that the resolve of the revisionist actor is paramount. Whether the response to gray zone conflict inhibits conflict (deterrence model) or enflames conflict (spiral model) depends on whether the initiator’s actions are influenced and motivated by previous rounds of deterrence success. The good news is this means that the seemingly novel forms of conflict short of war are little more than old wine in a new bottle. They do not require a sharp departure from current US strategy and instead require a recognition that modern gray zone conflict is a symptom of deterrence success that should be affirmed and reinforced rather than ignored and squandered.

# References

Acton, James M. “Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War.” *International Security* 43, no. 1 (August 1, 2018): 56–99.<https://doi.org/10.1162/isec_a_00320>.

Adams, Thomas K. “LIC (Low Intensity Clausewitz).” *Small Wars and Insurgencies* 1, no. 3 (December 1, 1990): 266–75.<https://doi.org/10.1080/09592319008422959>.

Altman, Dan. “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>.

Baezner, Marie, and Patrice Robin. “Cyber and Information Warfare in the Ukrainian Conflict.” Report. ETH Zurich, June 2017.<https://doi.org/10.3929/ethz-b-000169634>.

Bak, Daehee. “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>.

Bar-Siman-Tov, Yaacov. “The Strategy of War by Proxy.” *Cooperation and Conflict* 19, no. 4 (1984): 263–273.

Bennett, Andrew, 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>.

Blank, Stephen. “Russian Information Warfare as Domestic Counterinsurgency.” *American Foreign Policy Interests* 35, no. 1 (January 2013): 31–44.<https://doi.org/10.1080/10803920.2013.757946>.

Blaufarb, Douglas S. *The Counterinsurgency Era: U.S. Doctrine and Performance, 1950 to the Present*. Free Press, 1977.

Borghard, Erica D., 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>.

Boulding, Kenneth E. *Conflict and Defense: A General Theory*. New York: Harper, 1962.

Bragg, Belinda. “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>.

Branch, Jordan. “Spatial Metaphors and the Territorialization of Cybersecurity.” San Francisco, CA, 2018.

Brantly, A. F., 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>.

Brantly, Aaron F. “Cyber Actions by State Actors: Motivation and Utility.” *International Journal of Intelligence and CounterIntelligence* 27, no. 3 (September 1, 2014): 465–84.<https://doi.org/10.1080/08850607.2014.900291>.

Brecher, Michael, Jonathan Wilkenfeld, Kyle C. Beardsley, Patrick James, and David Quinn. “International Crisis Behavior Data Codebook.” Codebook, 2017.<http://sites.duke.edu/icbdata/data-collections/>.

Brodie, Bernard. “More About Limited War.” Edited by 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>.

Brown, Seyom. “Purposes and Pitfalls of War by Proxy: A Systemic Analysis.” *Small Wars & Insurgencies* 27, no. 2 (March 3, 2016): 243–57.<https://doi.org/10.1080/09592318.2015.1134047>.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press, 2016.

Carnegie, Allison, and Austin Carson. “The Spotlight’s Harsh Glare: Rethinking Publicity and International Order.” *International Organization*, May 2018, 1–31.<https://doi.org/10.1017/S0020818318000176>.

Carson, Austin. “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>.

———. *Secret Wars: Covert Conflict in International Politics*. Princeton Studies in International History and Politics. Princeton, NJ: Princeton University Press, 2018.

Carver, Michael. “Conventional Warfare in the Nuclear Age.” In *Makers of Modern Strategy from Machiavelli to the Nuclear Age.*, edited by Peter Paret, Gordon A Craig, and Felix Gilbert, 779–814. New Jersey: Princeton University Press, 1986.<http://public.eblib.com/choice/publicfullrecord.aspx?p=827816>.

Casey, Adam, and Lucan Ahmad Way. “Russian Electoral Interventions, 1991-2017.” Scholars Portal Dataverse, 2017.<https://doi.org/10.5683/SP/BYRQQS>.

Charap, Samuel. “The Ghost of Hybrid War.” *Survival* 57, no. 6 (November 2, 2015): 51–58.<https://doi.org/10.1080/00396338.2015.1116147>.

Chivvis, Christopher S. “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>.

Colby, Eldridge. “Against the Great Powers: Reflections on Balancing Nuclear and Conventional Power.” *Texas National Security Review* 2, no. 1 (November 2018).<https://tnsr.org/2018/11/against-the-great-powers-reflections-on-balancing-nuclear-and-conventional-power/>.

Copeland, Dale C. “Economic Interdependence and War: A Theory of Trade Expectations.” *International Security* 20, no. 4 (1996): 5–41.<https://doi.org/10.2307/2539041>.

Corbett, Julian. *Some Principles of Maritime Strategy*, 1911.

Danilovic, Vesna. “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>.

Davis, Joshua. “Hackers Take Down the Most Wired Country in Europe.” *Wired*, August 21, 2007.<https://www.wired.com/2007/08/ff-estonia/>.

Deibert, Ronald J., 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>.

DiResta, Renee, Kris Shaffer, Becky Ruppel, Robert Matney, Ryan Fox, Jonathan Albright, Ben Johnson, and Canfield Research. “The Tactics & Tropes of the Internet Research Agency.” Report for United States Senate Select Committee on Intelligence. New Knowledge, December 2018.

Downie, Richard D. “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>.

Drezner, Daniel W. “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>.

Driscoll, Jesse, 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>.

Driscoll, Jesse, and Zachary Steinert-Threlkeld. “Social Media and Russian Territorial Irredentism: Some Facts and a Conjecture.” Working Paper, 2019.

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

Early, Bryan, 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>.

Erickson, Andrew S., 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/>.

Fallon, Michael. “Speech Delivered by Secretary of State for Defence Sir Michael Fallon at the RUSI Landwarfare Conference.” Speech presented at the RUSI Landwarfare Conference, June 28, 2017.<https://www.gov.uk/government/speeches/rusi-landwarfare-conference>.

Fearon, James. “Bargaining Over Objects That Influence Future Bargaining Power.” Draft, October 1996.

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

Foust, Joshua. “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/>.

Freedman, Lawrence. “Ukraine and the Art of Limited War.” *Survival* 56, no. 6 (November 2, 2014): 7–38.<https://doi.org/10.1080/00396338.2014.985432>.

Freysinger, Robert C. “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>.

Friedman, Norman. *Seapower as Strategy: Navies and National Interests*. Naval Institute Press, 2001.

Fuhrmann, Matthew. “On Extended Nuclear Deterrence.” *Diplomacy & Statecraft* 29, no. 1 (January 2, 2018): 51–73.<https://doi.org/10.1080/09592296.2017.1420526>.

Gady, Franz-Stefan. “‘Little Blue Men:’ Doing China’s Dirty Work in the South China Sea.” Periodical. The Diplomat, November 5, 2015. http://thediplomat.com/2015/11/little-blue-men-doing-chinas-dirty-work-in-the-south-china-sea/.

Galeotti, Mark. “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>.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*. Hailer Publishing, 1964.

Ganguly, Sumit. “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>.

Gartzke, Erik. “The Capitalist Peace.” *American Journal of Political Science* 51, no. 1 (January 1, 2007): 166–91.<https://doi.org/10.1111/j.1540-5907.2007.00244.x>.

———. “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, Erik A., and Koji Kagotani. “Being There: U.S. Troop Deployments, Force Posture and Alliance Reliability.” Working Paper, 2017.

Gartzke, Erik, and Quan Li. “Measure for Measure: Concept Operationalization and the Trade Interdependence-Conflict Debate.” *Journal of Peace Research* 40, no. 5 (September 1, 2003): 553–71.<https://doi.org/10.1177/00223433030405004>.

Gartzke, Erik, 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>.

Gartzke, Erik, and Oliver Westerwinter. “The Complex Structure of Commercial Peace Contrasting Trade Interdependence, Asymmetry, and Multipolarity.” *Journal of Peace Research* 53, no. 3 (May 1, 2016): 325–43.<https://doi.org/10.1177/0022343316637895>.

Geers, Kenneth. *Cyber War in Perspective: Russian Aggression against Ukraine*. CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015.

———. “Cyberspace and the Changing Nature of Warfare.” SC Media US, August 27, 2008.<https://www.scmagazine.com/opinions/cyberspace-and-the-changing-nature-of-warfare/article/554872/>.

George, Alexander L., and Richard Smoke. “Deterrence and Foreign Policy.” *World Politics* 41, no. 2 (1989): 170–82.<https://doi.org/10.2307/2010406>.

———. *Deterrence in American Foreign Policy: Theory and Practice*. Columbia University Press, 1974.

George, Justin, 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>.

Goldsmith, Jack, and Tim Wu. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press, 2006.

Goldstein, Avery. “First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations.” *International Security* 37, no. 4 (April 1, 2013): 49–89.<https://doi.org/10.1162/ISEC_a_00114>.

Gompert, David C., and Martin Libicki. “Cyber Warfare and Sino-American Crisis Instability.” *Survival* 56, no. 4 (July 4, 2014): 7–22.<https://doi.org/10.1080/00396338.2014.941543>.

Götz, Elias. “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>.

Grant, Arthur V. “Strategic Decisions: The Mire of Low-Intensity Conflict.” *Comparative Strategy* 10, no. 2 (April 1, 1991): 165–75.<https://doi.org/10.1080/01495939108402840>.

Green, Michael, Kathleen Hicks, Zack Cooper, John Schaus, and Jake Douglas. *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*. Rowman & Littlefield, 2017.

Greenberg, Andy. “‘Crash Override’: The Malware That Took Down a Power Grid.” *Wired*, June 12, 2017.<https://www.wired.com/story/crash-override-malware/>.

———. “How An Entire Nation Became Russia’s Test Lab for Cyberwar.” *Wired*, June 20, 2017.<https://www.wired.com/story/russian-hackers-attack-ukraine/>.

———. “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/>.

Hammond, Grant T. “Low Intensity Conflict: War by Another Name.” *Small Wars & Insurgencies* 1, no. 3 (December 1, 1990): 226–38.<https://doi.org/10.1080/09592319008422957>.

Hart, Sir Basil Henry Liddell. *Strategy: The Indirect Approach*. Faber & Faber, 1954.

Howard, Philip N, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. “The IRA, Social Media and Political Polarization in the United States, 2012-2018.” Working Paper. Oxford, UK: Computational Propaganda Research Project, 2018.

Huth, Paul, and Bruce Russett. “Deterrence Failure and Crisis Escalation.” *International Studies Quarterly* 32, no. 1 (1988): 29–45.<https://doi.org/10.2307/2600411>.

Jackson, Van. “Preventing Nuclear War with North Korea.” *Foreign Affairs*, September 11, 2016.<https://www.foreignaffairs.com/articles/north-korea/2016-09-11/preventing-nuclear-war-north-korea>.

———. “Tactics of Strategic Competition: Gray Zones, Redlines, and Conflict before War.” *Naval War College Review* 70, no. 3 (2017): 39–61.

Jensen, Benjamin, 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>.

Jervis, Robert. “Cooperation Under the Security Dilemma.” *World Politics* 30, no. 2 (1978): 167–214.<https://doi.org/10.2307/2009958>.

———. *Perception and Misperception in International Politics*. Vol. 49. Princeton, N.J: Princeton University Press, 1976.

———. *The Illogic of American Nuclear Strategy*. Cornell University Press, 1984.

Johnson, Loch K. “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>.

———. “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/>.

Joubert, Vincent. “Five Years after Estonia’s Cyber-attacks: Lessons Learned for NATO?” NATO Defense College, 2012. JSTOR.<https://www.jstor.org/stable/resrep10366>.

Kalyvas, Stathis. “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>.

Kapur, S. Paul. *Dangerous Deterrent: Nuclear Weapons Proliferation and Conflict in South Asia*. Stanford University Press, 2007.

Kennan, George. “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>.

Kilcullen, David. *Counterinsurgency*. Hurst, 2010.

Kinross, Stuart. “Clausewitz and Low-Intensity Conflict.” *Journal of Strategic Studies* 27, no. 1 (March 1, 2004): 35–58.<https://doi.org/10.1080/0140239042000232765>.

Kissinger, Henry A. “Military Policy and Defense of the ‘Grey Areas.’” *Foreign Affairs* 33, no. 3 (1955): 416–28.<https://doi.org/10.2307/20031108>.

———. “Strategy and Organization.” *Foreign Affairs* 35, no. 3 (1957): 379–94.<https://doi.org/10.2307/20031235>.

Kitson, Frank. *Low Intensity Operations: Subversion, Insurgency, Peace-Keeping*. Faber & Faber, 1971.

Kober, Avi. “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>.

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer. “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>.

Kornbluh, Peter, 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>.

Kostyuk, Nadiya, and Yuri M. Zhukov. “Invisible Digital Front: Can Cyber-attacks Shape Battlefield Events?” *Journal of Conflict Resolution* 63, no. 2 (2019): 317–47.<https://doi.org/10.1177/0022002717737138>.

Lanoszka, Alexander. “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>.

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

Lepgold, Joseph, 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>.

Lieberman, Elli. *Reconceptualizing Deterrence: Nudging Toward Rationality in Middle Eastern Rivalries*. Routledge, 2012.

Lindsay, Jon R. “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>.

———. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies* 22, no. 3 (July 1, 2013): 365–404.<https://doi.org/10.1080/09636412.2013.816122>.

———. “Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack.” *Journal of Cybersecurity* 1, no. 1 (September 1, 2015): 53–67.<https://doi.org/10.1093/cybsec/tyv003>.

Lindsay, Jon R., and Erik Gartzke. “Coercion through Cyberspace: The Stability-Instability Paradox Revisited.” In *Coercion: The Power to Hurt in International Politics*, edited by Kelly M. Greenhill and Peter Krause. New York, NY: Oxford University Press, 2018.

———, eds. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. 1st edition. New York, NY: Oxford University Press, 2019.

Lin-Greenberg, Erik. “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>.

Marten, Kimberly. “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>.

———. “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>.

Matláry, Janne Haaland. “Partners versus Members? NATO as an Arena for Coalitions.” In *NATO’s Post-Cold War Politics: The Changing Provision of Security*, edited by Sebastian Mayer, 251–66. New Security Challenges Series. London: Palgrave Macmillan UK, 2014.<https://doi.org/10.1057/9781137330307_14>.

Maxwell, David. Gray Zone Subject Matter Expert Interview. Interview by Sarah Canna, June 14, 2016.

Mazarr, Michael. “Mastering the Gray Zone: Understanding a Changing Era of Conflict.” Monogram, February 2, 2015.<http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1303>.

Metz, Steven. “Foundation for a Low Intensity Conflict Strategy.” *Comparative Strategy* 8, no. 2 (January 1989): 265–73.<https://doi.org/10.1080/01495938908402780>.

Nagl, John A. *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam*. University of Chicago Press, 2005.

Noetzel, Timo, and Benjamin Schreer. “Does a Multi-Tier NATO Matter? The Atlantic Alliance and the Process of Strategic Change.” *International Affairs* 85, no. 2 (March 1, 2009): 211–26.<https://doi.org/10.1111/j.1468-2346.2009.00790.x>.

Nye, Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (January 1, 2017): 44–71.<https://doi.org/10.1162/ISEC_a_00266>.

Office of the Deputy Attorney General. “Appointment of Special Counsel to Investigate Russian Interference with the 2016 Presidential Election and Related Matters.” Washington, DC, May 17, 2017.<https://www.justice.gov/opa/press-release/file/967231/download>.

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>.

Olson, William. “The Concept of Small Wars.” *Small Wars & Insurgencies* 1, no. 1 (April 1, 1990): 39–46.<https://doi.org/10.1080/09592319008422940>.

Oneal, John R., and Bruce Russett. “Assessing the Liberal Peace with Alternative Specifications: Trade Still Reduces Conflict.” *Journal of Peace Research* 36, no. 4 (July 1, 1999): 423–42.<https://doi.org/10.1177/0022343399036004003>.

O’Rourke, Lindsey A. *Covert Regime Change: America’s Secret Cold War*. Cornell Studies in Security Affairs. Ithaca, NY: Cornell University Press, 2018.

Osgood, Robert E. “The Reappraisal of Limited War.” *The Adelphi Papers* 9, no. 54 (February 1969): 41–54.<https://doi.org/10.1080/05679326908448127>.

Paul, Christopher, 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.

Petersen, Roger D. *Resistance and Rebellion: Lessons From Eastern Europe*. Cambridge: Cambridge University Press, 2001.<https://doi.org/10.1017/CBO9780511612725>.

Powell, Robert. “Nuclear Brinkmanship, Limited War, and Military Power.” *International Organization* 69, no. 03 (June 2015): 589–626.<https://doi.org/10.1017/S0020818315000028>.

Poznansky, Michael, and Evan Perkoski. “Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution.” *Journal of Global Security Studies*, September 2018.<https://doi.org/10.1093/jogss/ogy022>.

Raghavan, V.R. “Limited War and Nuclear Escalation in South Asia.” *The Nonproliferation Review* 8, no. 3 (September 2001): 82–98.<https://doi.org/10.1080/10736700108436865>.

Rauchhaus, R. “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>.

Raymond, Mark. “Puncturing the Myth of the Internet as a Commons,” 2013.

Rosen, Stephen Peter. “Vietnam and the American Theory of Limited War.” *International Security* 7, no. 2 (1982): 83–113.<https://doi.org/10.2307/2538434>.

Rovner, Joshua, Jon R. Lindsay, Kimberly Marten, and Lindsey A. O’Rourke. “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>.

Russell, Richard L. “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>.

Sagan, Scott Douglas, and Kenneth Neal Waltz. *The Spread of Nuclear Weapons: A Debate Renewed*. Norton, 2003.

Santoro, David, 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/>.

Schelling, Thomas C. *Arms and Influence*. Yale University Press, 1966.

———. “Bargaining, Communication, and Limited War.” *Conflict Resolution* 1, no. 1 (1957): 19–36.

Schmidt, Andreas. “The Estonian Cyberattacks.” In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, edited by Jason Healey, 174–93. Cyber Conflict Studies Association, 2013.

Schneider, Jacquelyn. “Deterrence in and through Cyberspace.” In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by Jon R. Lindsay and Erik Gartzke, 1st edition. New York, NY: Oxford University Press, 2019.

———. *The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict*. ProQuest LLC, 2017.

Schram, Peter. “Hassling.” Working Paper, 2019.

Schultz, George. “Low-Intensity Warfare: The Challenge of Ambiguity.” Conference Address presented at the Low-Intensity Warfare Conference, National Defense University, Washington, DC, January 15, 1986.<https://www.jstor.org/stable/pdf/20692938.pdf>.

Shakarian, Paulo. “The 2008 Russian Cyber Campaign against Georgia.” *Military Review* 91, no. 6 (November 1, 2011): 63.

Shapiro, Jacob N. *The Terrorist’s Dilemma: Managing Violent Covert Organizations*. Princeton University Press, 2013.

Shy, John, and Thomas W. Collier. “Revolutionary War.” In *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, edited by Peter Paret, Gordon A Craig, and Felix Gilbert, 815–62. New Jersey: Princeton University Press, 1986.

Sides, John, 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.

Singer, David J, Stuart Bremer, and John Stuckey. “Capability Distribution, Uncertainty, and Major Power War, 1820-1965.” In *Peace, War, and Numbers*, by Bruce M. Russett, 19–48. Sage Publications, 1972.

Slayton, Rebecca. “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>.

Smith-Spark, Laura, 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>.

Snyder, Glenn. “The Balance of Power and the Balance of Terror.” In *World in Crisis: Readings in International Relations*, edited by Frederick Hartmann, 180–91. New York: The Macmillan Company, 1965.

Snyder, Glenn Herald. *Deterrence and Defense*. Princeton University Press, 1961.

Sobek, David, 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>.

Sowell, Jesse H. “Finding Order in a Contentious Internet.” Thesis, Massachusetts Institute of Technology, 2015.<http://dspace.mit.edu/handle/1721.1/97324>.

Stein, Janice Gross. “Calculation, Miscalculation, and Conventional Deterrence.” In *Psychology and Deterrence*, by Richard Ned Lebow and Robert Jervis. JHU Press, 1989.

Sullivan, Patricia L. “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>.

Taber, Robert. *War of the Flea: The Classic Study of Guerrilla Warfare*. L. Stewart, 1965.

Thomas, Timothy. “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>.

Thomas, Timothy L. “Manipulating the Mass Consciousness: Russian And Chechen ‘Information War’ Tactics In The 2nd Chechen-Russian Conflict.” FMSO Monographs. Foreign Military Studies Office, August 1, 2000.<https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/243758>.

Thompson, Sir Robert Grainger Ker. *Defeating Communist Insurgency: The Lessons of Malaya and Vietnam*. F. A. Praeger, 1966.

Traynor, Ian. “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>.

Turbiville, Graham H. “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>.

Tyler, Patrick E. “A Talkative Putin Demonstrates Value of Cyberspace.” *The New York Times*, March 7, 2001, sec. World.<https://www.nytimes.com/2001/03/07/world/a-talkative-putin-demonstrates-value-of-cyberspace.html>.

Ucko, David H. *The New Counterinsurgency Era: Transforming the U.S. Military for Modern Wars*. Georgetown University Press, 2009.

US Army. “Army Field Manual 3-24: Counterinsurgency,” November 30, 2006.<https://www.hsdl.org/?abstract&did=>.

Valeriano, Brandon, and Ryan C. Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press, 2015.

Valeriano, Brandon, and Ryan C Maness. “The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11.” *Journal of Peace Research* 51, no. 3 (May 1, 2014): 347–60.<https://doi.org/10.1177/0022343313518940>.

Votel, Joseph, Charles Cleveland, Charles Connett, and Will Irwin. “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>.

Wagner, R. Harrison. “Bargaining and War.” *American Journal of Political Science* 44, no. 3 (2000): 469–84.<https://doi.org/10.2307/2669259>.

Warden, John. “Limited Nuclear War: The 21st Century Challenge for the United States.” Livermore Papers on Global Security. Lawrence Livermore National Laboratory: Center for Global Security Research, July 2018.

Wood, Elisabeth Jean. *Insurgent Collective Action and Civil War in El Salvador*. Cambridge University Press, 2003.

Woodman, Dr Stewart. “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>.

Yeeson, Erik. “NATO and Russia in Kosovo.” *Perspectives*, no. 13 (1999): 11–19.

Zhang, Jiakun Jack. “Is China an Exception to the Commercial Peace?” Dissertation, UC San Diego, 2018.

1. The authors wish to thank the members of the Center for Peace and Security Studies (cPASS), particularly 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. [↑](#footnote-ref-1)
2. In the theatrical metaphor used by Austin Carson (2018), covert action on the “backstage” of politics and collusion to maintain a fiction on the “frontstage” facilitated escalation control. [↑](#footnote-ref-2)
3. Many commentators have focused on the fact Ukraine was not part of NATO, inferring that the Russian incursion is not technically a deterrence failure. The salient issue is how Russia intervened, however, which both reflects the effect of possible NATO intervention and the simultaneous shaping of actions in response to this risk. [↑](#footnote-ref-3)
4. Data by Kostyuk and Zhukov (2019) is too narrowly focused for our analysis (cyber-attacks in Ukraine). [↑](#footnote-ref-4)
5. The only country-year that appears in both datasets is Ukraine 2014. We standardized codings across the two datasets using variable definitions from respective codebooks. A severity less than or equal to 2 in DCID’s coding is synonymous in our recoding with REI’s coding for disinformation, a severity between 3 and 7 equals REI’s coding for cyberattack, and no cases in DCID have a severity greater than 7. We adopted Valeriano and Maness (2014)’s approach of sampling on intensity when there are multiple observations in a given time unit. [↑](#footnote-ref-5)
6. 5 ICB cases from 1994-2015 identify Russia as the conflict initiator. 3 of these (Georgia 2002, Georgia 2004, and Syria 2015) are not included in either DCID or REI and are thus uniquely added cases. [↑](#footnote-ref-6)
7. The first two variables, information operations and cyber disruption, were coded using the same coding protocol and codebook definitions as the DCID and REI datasets to ensure the coding is comparable. However, they were coded without reference to the coding in prior datasets to maintain consistency across the newly aggregated data. A comparison of the coding decisions as well as list of original sources can be found in the replication file. [↑](#footnote-ref-7)
8. 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 is also likely to lack sympathetic populations and local knowledge in “contested zones” far from home (Posen 2003). The loss of strength can be partially offset by basing and mobility (Corbett 1911; Friedman 2001). [↑](#footnote-ref-8)
9. 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. [↑](#footnote-ref-9)
10. A botnet is a network of compromised computers that can be controlled remotely, in this case amplifying the traffic directed at targeted servers to overwhelm its capacity to accept connections. [↑](#footnote-ref-10)
11. General deterrence discourages states from making challenges in the first place, as distinguished from immediate deterrence which responds to explicit challenges (Huth and Russett 1988). [↑](#footnote-ref-11)