After Deterrence: Explaining Conflict Short of War

December 2019

Russia’s intervention in Ukraine is a form of limited conflict in the “gray zone” between peace and war. Some wars are limited because at least one belligerent has only limited means. Gray zone conflict, by contrast, involves strong nation-states that have plenty of means but limited ends. Capable actors might employ only a subset of their capabilities for the sake of efficiency if their objectives require only limited means. Alternatively, voluntary limits may reflect concerns about the potential risks of escalation. Actions in the gray zone thus pose a discrimination problem: aggressors motivated by efficiency are more inclined to escalate if challenged, while aggressors concerned about deterrence should tend to back down. Indeed, if gray zone conflict is a reaction to deterrence, its scope and intensity should vary inversely with the credibility of deterrence. Drawing on Russian aggression, we find support for the deterrence hypothesis in qualitative and quantitative data. Gray zone conflict can be interpreted as a symptom of successful deterrence rather than evidence of deterrence failure.

Word Count: 13263 (excluding footnotes)

# Introduction

In the wake of the overthrow of Ukrainian President Viktor Yanukovych in February 2014, the Crimean Peninsula was invaded by “little green men,” soldiers whose uniforms lacked insignia or other identifying information. While nobody seriously doubted the origin of these troops, the pretext of anonymity afforded NATO a fig leaf—had it needed one—to avert direct confrontation between West and East.[[1]](#footnote-2) The Kremlin formally annexed Crimea shortly thereafter. Russian intervention in Ukraine continues to this day, consisting of limited ground operations and aggressive cyber campaigns (Angevine et al. 2019). Many now worry about a potential repeat performance in the Baltics, where ethnic Russian minorities and NATO membership make for a dangerous mix. Other Russian “active measures” similarly appear to be designed to undermine the legitimacy of Western democratic institutions and to inflame a wave of nationalist populism opposed to the “liberal international order,” while ensuring that military confrontation between Russia and NATO does not take place (Paul and Matthews 2016).

According to former British Defense Secretary Michael Fallon, “That is not a Cold War. It is a grey war. Permanently teetering on the edge of outright hostility. Persistently hovering around the threshold of what we would normally consider acts of war” (Fallon 2017). The imagery of little green men in “the gray zone” has also been extended to “little blue men” used by China to erode “red lines” in maritime East Asia (Green et al. 2017). The kaleidoscopic language highlights both practical and conceptual challenges in the practice of deterrence. As the Chairman of the Joint Chiefs of Staff noted, “Our traditional approach is either we’re at peace or at conflict. And I think that’s insufficient to deal with the actors that actually seek to advance their interests while avoiding our strengths” (Dunford 2016).

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

The good news in our interpretation is that gray zone conflict is a response to deterrence success. We expect the severity of gray zone conflict to be attenuated wherever the defender’s power and resolve are higher. The bad news is that gray zone conflict probes the threshold of deterrence effectiveness. Thus, we expect conflict severity to be greater where defender power and resolve is more questionable. A nation’s interests tend to vary across different issue areas, as does its ability to project military power to back up deterrent threats. Therefore, we expect the intensity and lethality of conflict to vary along a gradient of deterrence credibility, analogous to the military loss of strength gradient across geographical distance (Boulding 1962). We test this hypothesis by drawing on a new dataset of Russian interventions since the end of the Cold War and qualitative studies of Russia’s major cyber campaigns, which vary in the additional types of force that Russia has mobilized. We find that Russia systematically limits its choice of military means along an East-West gradient, behaving more furtively as Western credibility increases.

Deterrence shapes the way that conflict emerges, but it cannot suppress conflict altogether. An adversary is seldom passive. There will always be attempts at end-runs or push-back, even when deterrence is credible. It is also important to avoid overextending commitments where credibility is in doubt. Policymakers should be sensitive to the deterrence gradient, seeking to reinforce success and respect weakness. We make our argument in four parts. First, we locate gray zone conflict in the broader literature on limited war. Second, we analyze limited conflict through the lens of deterrence theory. Third we conduct a plausibility probe of our argument using recent Russian cases. We conclude with implications of our argument.

# Between Peace and War

There is nothing new about conflict that falls ambiguously between peace and war. There is a long history of, and a vast literature on, limited conflict (Kissinger 1955; Osgood 1969), salami tactics (Schelling 1966), low intensity conflict (Turbiville 2002), revolutionary war (Shy and Collier 1986), military operations other than war (Kinross 2004), covert operations (Carson 2018; O’Rourke 2018), small wars (Olson 1990), and proxy wars (Driscoll and Maliniak 2016). Many (but not all) of these concepts emphasize asymmetric struggles with combatants that are unable in material terms to fight on a larger scale or with higher intensity.

The interesting puzzle about gray zone conflict, as we will use the term here, is that adversaries are able but *unwilling* to broaden the scope or intensity of a military engagement. But this is also not new. In 1978, Kissinger advocated for an intelligence community that could “defend the American national interest in the gray areas where military operations are not suitable and diplomacy cannot operate” (Johnson 2013). General Votel has described the Cold War as “a 45-year-long Gray Zone struggle” in which the United States and Soviet Union conducted proxy wars, covert operations, and (dis)information campaigns while avoiding a direct military and likely nuclear confrontation (Votel et al. 2016). Cold War deterrence shaped the modality and severity of conflict, but it did not, and could not, eliminate it completely. Today many are concerned about an emerging manifestation of limited war, often called “gray zone conflict.” United States Special Operations Command (SOCOM) has defined it as:

a conceptual space between peace and war occurring when actors purposefully use single or multiple elements of power to achieve political-security objectives with activities that are typically ambiguous or cloud attribution and exceed the threshold of ordinary competition, yet intentionally fall below the level of large-scale direct military conflict and threaten US and allied interests by challenging, undermining, or violating international customs, norms, or laws. (Bragg 2017)

Again, this is not a new problem. While it is convenient to think of peace and war as dichotomous, discrete outcomes, observers have long recognized that tension and violence exist on a spectrum, even as the language used to describe it evolves (Lebow 2010). 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 (wars limited by ends), conventional war in the shadow of nuclear weapons (wars limited by risks), and low-intensity conflict with irregular forces (wars limited by means).

## Wars Limited by Ends

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

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 (Kennan 1948).

The emphasis on limited political objectives over military operations represented an important shift in thinking. The Korean War exemplified an underappreciated type of war fought to achieve political ends short of traditional military victory despite having the capability to do so (Osgood 1969). Contemporary treatment understood limited war as a conflict between actors who had the capacity to increase battlefield commitment but did not want to do so, creating a third option short of major war yet beyond acquiescence (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 or limiting the geographic scope of conflict (Woodman 1991). This form of war required some degree of tacit agreement or common conjecture among adversaries to limit the scope of war. During the Vietnam war, for instance, the North Vietnamese leadership was prepared to escalate conflict even as China and the Soviet Union worked to restrain their ally (Carver 1986).

## Wars Limited by Risk

Cold War strategists advanced the notion of “the stability-instability paradox” to explain how incentives for engaging in conflict at lower levels of intensity or in peripheral theaters arise out of disincentives for initiating nuclear war (or even major conventional war) (Jervis 1984). According to Snyder, “nuclear technology introduced a new form of intent-perception and a new form of uncertainty — that concerning what types of military capability the opponent was likely to use and what degree of violence he was willing to risk or accept” (Snyder 1965). The presence of nuclear weapons might prevent world war, but it could simultaneously encourage localized aggression or smaller, more limited conflicts (Sagan and Waltz 2003). At the same time, the feasibility of “weakening the enemy with pricks instead of blows” is limited by the implicit risk of nuclear escalation (Hart 1954). Modern studies evaluate stability-instability quantitatively or in specific regions (Ganguly 1995; Rauchhaus 2009).

Recent formalizations of limited conflict in the shadow of major war point to the need for updated conceptions of deterrence. Schelling argued that “the main consequence of limited war, and potentially a main purpose for engaging in it, is to raise the risk of larger war” (Schelling 1966). Gray zone conflict poses a different relationship in which a capable actor may choose to engage in limited war precisely to *lower* the risk of larger war (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.

Deterrence is really a strategy designed to buy time against an adversary committed to changing the status quo. George and Smoke raise the issue of “designing around” deterrence as adversaries seek out options that “offers an opportunity for gain while minimizing the risk of an unwanted response by the defender” (A. George and Smoke 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 remains a perverse symptom of its success so long as the adversary limits its means and aims, even in cases where the target panics or misperceives that the attacker has expansive aims (as Israel did). Lieberman thus argues that “designing around” is a sign of deterrence success if an adversary shapes its challenge in response to the anticipated reaction of the defender (Lieberman 2012).

## Wars Limited by Means

The Cold War also witnessed numerous decolonization struggles and proxy wars in the Third World. Limited war with irregular forces rather than a peer competitor directly garnered much attention in the 1970s under the rubric of “low intensity conflict” (LIC) (Schultz 1986). Some treatments of LIC focus on the use of light weapons and ambush tactics (Kornbluh and Hackel 1986) while others identify the phenomenon in terms of non-state actors (Kinross 2004). Unsurprisingly LIC is more prevalent in under-developed or poorly institutionalized regions (Hammond 1990). The classical literature on counterinsurgency (Galula 1964; Taber 1965) and its modern variants (Nagl 2005; Kilcullen 2010) fall into this category.

Wars with means-limited actors have received most of the attention after the Cold War as the United States has been involved in a long series of peacekeeping operations and grueling counterinsurgencies. A vast academic literature on civil war has emerged in recent years to explain the behavior, motives, and organizational structure of irregular actors (Petersen 2001; Wood 2003) and the militaries that fight them (Hazelton 2017). The recent renewal of interest in low-intensity conflict between more capable competitors in many ways represents a return to the two earlier themes—wars limited by ends and risk-sensitivity.

## Modern Gray Zone Conflict

Gray zone conflict today has been described as “a carefully planned campaign operating in the space between traditional diplomacy and overt military aggression” employed by revisionist states with grand geopolitical ambitions and irresistible capabilities (Mazarr 2015). This pessimism has even led some to advocate revamping deterrence to focus on threats from the gray zone (Matisek 2017). Russia, and its intervention in Ukraine in particular, is the paradigmatic exemplar (Marten 2015). Russia uses novel forms of “hybrid warfare” to facilitate increased aggression against NATO and the West (Chivvis 2017). This view holds that aggressors can work around adversaries’ red lines to achieve coercive bargaining success without triggering escalation (Altman 2018). If so, we might expect to see Russia engaging in gray zone conflict in as many situations as possible; there is little reason to avoid undertaking an efficient form of warfare that provides significant gains at low cost.

The familiar logic of the stability-instability paradox plays out today with different, usually lower, thresholds. Deterrence now results as much from the risk of escalation to major conventional war, or even economic disruption, as from the threat of nuclear conflagration. One potential novelty, however, exists in the growing diversity of means by which low intensity conflict can be practiced (Wirtz 2017). The emergence of new, cheaper implements of coercion have made it easier than before to fight circumspect contests (Lindsay and Gartzke 2018).

Even sceptics of the potency of new information technologies highlight the expanded repertoire of military strategies available for low intensity conflict, especially online espionage and cyber disruption (Rid 2013; Jensen, Valeriano, and Maness 2019). Compared to historical subversions this is certainly true. Yet there are also more, and more technologically sophisticated, means available for all types of warfare, some of which are only likely to be used in major war (e.g., anti-satellite weapons, hypersonic munitions, anti-ship ballistic missiles). The apparent expansion of the number and type of means observed in many conflicts in fact reflects a reduction of the range of possible means that belligerents might employ for deterrence and war. It is important not to conflate the increasing variety of tools available for conflicts of *all* types with the use of a *subset* of means for limited conflict. Cyber operations may be prevalent in the gray zone, but they will be prevalent in every war of the 21st century.

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

The ironic fact is, these new and elusive challenges have proliferated, in part, because of our success in deterring nuclear and conventional war. Our adversaries know they cannot prevail against us in either type of war. So they have done the logical thing: they have turned to other methods. Low-intensity warfare is their answer to our conventional and nuclear strength a flanking maneuver, in military terms (Schultz 1986).

Our theory hopes to reemphasize this optimism concerning the motivations underlying gray zone conflict. The phenomenon of gray zone conflict is not new, but its causes have evolved in a way that should encourage patience before sounding alarms.

# A Theory of Gray Zone Conflict

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

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

Second, gray zone conflict involves *capable initiators*. In order to limit one’s means, an actor must have a portfolio of means to choose from. This differentiates Russian or American special operations forces from insurgents, even in cases where their tactics appear similar. Moreover, weaker states and rebel groups vary considerably in their war aims and thus may refrain from giving their maximum effort (Staniland 2012).

Third, gray zone conflict must be preferred *by both sides* in a contest. Capable belligerents have the capability to escalate but they choose not to. The target would rather have the opponent engage in gray zone conflict than engage in overt warfare as a result of the target’s reaction to the provocation. Anticipating this, the attacker selects technologies that deliberately obfuscate its intentions or complicate attribution. This is done for the benefit of the target, to relieve it from an obligation to respond forcefully to provocation, rather than for the benefit of the initiator, to enable it to escape retaliation. Tacit collusion between adversaries enables them to avoid mutually harmful escalation (Carson 2016; 2018).

## A Typology of Limited Conflict

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

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

**Table 1**: A Typology of Limited Conflict

Powerful actors that are highly resolved to revise the status quo will tend to use as much force as needed to get the job done. A unilateral preference for conquest makes major combat operations attractive, where force is limited simply as a function of the local balance of power. More resistance can always be met with more force, but overkill wastes resources unnecessarily. If capable actors only have modest ambitions, moreover, they will be more willing to settle for less and to employ less effective modes of operation. Voluntary limitation of means enables an aggressor to minimize both costs *and* risk exposure. The voluntary limitation of ends allows the target to keep more of what it already has. Escalation in this situation is thus mutually undesirable. In order to limit the risk of escalation, gray zone actors voluntarily limit the means they use to pursue their limited ends.

The Iraq War illustrates all four categories. The U.S.-led Coalition invaded Iraq in 2003 with less than 180,000 troops even though the United States could have mobilized hundreds of thousands more. Major combat operations in Iraq were limited by a desire to cut costs, not concerns about deterrence. As subsequent events made clear, American politicians ignored the significant and arguably foreseeable costs of occupation.[[2]](#footnote-3) Throughout the next decade the U.S. military battled a mixture of foreign jihadists and local militias. While insurgent groups used similar means—improvised explosive devices and ambush attacks—their aims differed. Jihadists sought the revolutionary transformation of Iraqi society. Militias sought to control local areas and economies. Coalition Forces struggled with both groups before learning how to defeat the former (with the counterterrorism methods of Joint Special Operations Command) and to coopt the latter (by striking deals with the Anbar Awakening and similar movements) (Gordon and Trainor 2007; Lindsay and Petersen 2012). Had American policymakers appreciated the true costs of their war, they would have faced a choice between two alternatives. If they were indeed resolved to conquer Iraq, they could have increased force levels to enable both invasion and stabilization. That is, they could have conducted major combat operations with a larger set of means and resources. The troop surge of 2008 followed a similar logic by increasing resources in an attempt to transform Iraq into a stable liberal society. If, however, policymakers’ war aims were more limited, they might have sought an alternative to invasion, such as maintenance of the existing containment regime. Indeed, between 1991 and 2003, the United States engaged in a continuous gray zone contest to contain Saddam Hussein with air policing, economic sanctions, covert intelligence, and occasional air strikes. The Baathist regime survived while the United States avoided a costly ground war, outcomes that were mutually preferable for both sides compared to the, at that time anticipated outcome of the war. The exogenous shock of the 9/11 terrorist attacks then raised concerns for some policymakers about the long-term viability of containment. In other words, the desire for gray zone was no longer mutual.

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

## The Escalation Dilemma

Given that capable actors may use limited means for limited ends for quite different reasons, the label of “major combat operations” may be a misleading way to describe conflict motivated by efficiency.[[3]](#footnote-4) A challenger who is patient and capable relative to its adversaries at low intensities might benefit by choosing a very limited conflict strategy. While high intensity conflict may be able to accomplish an aggressor’s goals, it may also be unnecessary and inefficient if victory can be achieved with lower cost at lower levels of dispute intensity (Altman 2018). If the local balance of power greatly favors the initiator, then it may only need to employ modest resources to get all that it seeks in a reasonable timeframe. If the aggressor only needs a few special operations units and some cyber effects to overwhelm the enemy, then a contest may be observably indistinguishable from the prototypical gray zone conflict. This sort of indistinguishability is most likely in cases where the revisionist actor has limited aims but values them greatly, i.e., it desires something well short of total conquest but only needs to mobilize a small number of forces to compel the other side to make concessions.

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

Limited conflict ≿Ordinary competition ≿High intensity warfare

Limited conflict ≿High intensity warfare ≿Ordinary competition

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

This situation recapitulates the basic logic of the security dilemma (Jervis 1978). The classic problem is to divine whether a state is satisfied with the status quo or has revisionist intentions. The spiral model applies to the former while the deterrence model applies to the latter; applying the wrong model leads to tragic escalation (threatening status quo seekers) or preventable exploitation (appeasing revisionists). The difference here is that the gray zone actor is already known to be revisionist; the uncertainty is thus more about its resolve than its interest. In security dilemma logic, escalation occurs when the deterrence model is (inappropriately) applied to a status quo actor (but not to the revisionist). In gray zone logic, escalation occurs when the deterrence model is applied to a more resolved revisionist (but not to the less resolved aggressor). If the problem of the security dilemma is to decide *whether* to deter, the problem of the gray zone is to decide *how much*. Even if all actors are assumed to harbor revisionist ambitions, security dilemma-like dynamics still apply in determining the ways in which they are deterred from given behaviour (Schweller 1996).

## The Deterrence Gradient

If conflict varies continuously between peace and war, then it might be explained by treating deterrence success and failure as continuously variable. If gray zone conflict is a second-best reaction to successful deterrence, then conflict severity should be inversely proportional to the credibility of deterrence. Conflict motivated by efficiency should not be so correlated. Furthermore, conflict at the weaker end of the deterrence gradient should be more motivated by efficiency concerns than fears about retaliatory consequences.

To operationalize this hypothesis, we posit a deterrence analogue to the military loss of strength gradient (Boulding 1962). All things being equal, a state requires more supplies and troops to achieve the same concentration of force further from its border. Distant deployments involve extended supply lines and exposed flanks. An army may also lack sympathetic populations and local knowledge in “contested zones” far from home (Posen 2003). The loss of strength can be partially offset by basing and mobility but not eliminated due to the enduring vulnerabilities of naval power and frictions with host nations (Corbett 1911). Geography is not the focus of this article, per se, but we use it here to instrument variation in the strength of deterrence. This in turn enables us to examine arguments about the relationship between deterrence and gray zone conflict. We do not assume that geography causes deterrence directly, but it can be used as a convenient proxy for other factors that do.

Insofar as military power is affected by a loss of strength gradient, deterrence that relies on military power should also decay in distance. There are other reasons to expect resolve to be affected by proximity. All things being equal, states likely care more about regional issues that more directly affect their populations than about happenings far from home. Defenders will thus be more resolved to resist aggression on their borders, while attackers campaigning from distant shores will are less so. Alliances with neighboring states should similarly be more credible since patrons are generally more willing to defend a proximate client (Bak 2018). Conversely, commitments should be less credible with distance as well, as patrons will fear entrapment by distant allies who have stronger local interests (Christensen and Snyder 1990). While NATO security guarantees nominally cover all 29 member states equally, the 12 founding members in Western Europe and North America are arguably more confident in this commitment (J. George and Sandler 2018). Indeed, recent Eastern European entrants have questioned NATO resolve. Eastern European members also appear to have greater need of protection, given that Russia is both more interested in, and better able to control, territory near its borders (Matláry 2014).

Technology conditions but does not eliminate geography. Although it seems cyberspace has opened up the world to anyone with an internet connection, most states can and do enforce their laws on the digital infrastructure located within their borders (Goldsmith and Wu 2006). Indeed, cyber conflict appears to be concentrated along the fissures of traditional geographic rivalries. To the extent that cyberspace does enable remote conflict, we should expect it to be used for limited aims operations that do not directly threaten vital interests. Because cyber-attacks rarely lead to escalation, the cyber domain is particularly attractive for risk-sensitive revisionists (Schneider 2017). The cybersecurity literature offers two reasons for the empirical pattern of restraint observed in the cyber domain, and geography plays a tacit role in both (Valeriano and Maness 2014). First, complex offensive cyber operations require detailed intelligence preparation, often including human intelligence (Slayton 2017).[[4]](#footnote-5) Intelligence is harder to collect and understand from a distance, and poor intelligence enhances cyber deterrence-by-denial. Second, attribution and retaliation depend on capabilities in more traditional domains (Lindsay 2013; Gartzke and Lindsay 2015). Thus deterrence-by-punishment of cyber aggression will be affected by the same loss-of-strength gradient that affects cross-domain military capabilities in the terrestrial world. In sum, we expect Western resolve and capability to decrease from West to East while Russian resolve and capability increases.

## A Note on Third Parties

As the logic of our argument is dyadic, the role of third parties deserves a brief comment. Many treatments of covert warfare focus on military aid to local proxies from a powerful patron. As an analytical first cut, a complex portfolio of actors can be simplified as a dyadic pairing in gray zone conflict.[[5]](#footnote-6) That is, a target’s allies can be treated as part of the target’s capabilities, discounted by the level of commitment (or disunity) in an alliance. Lanoszka argues that a gray zone initiator must have escalation dominance over the target, e.g., Russia has more capability at every rung of the escalation ladder than Ukraine or Lithuania (Lanoszka 2016). His argument appears to run counter to our deterrence story until the weaker state is considered together with its powerful protector(s). Russia may not be deterred by the Ukrainian military directly, but it calibrates its actions to avoid triggering a confrontation with NATO. More actors may be considered “capable” in this sense than if assessed in purely bilateral terms.

Importantly, alliances, commitment mechanisms, and other attempts to aggregate capabilities are often explicitly or implicitly designed to generate deterrence by reducing agency (autonomy) on the part of individual participants, making them behave more like a single unit (Sobek and Clare 2013). Deterrence works if an ally might respond to a given provocation, but friction between them complicates deterrence effectiveness (Danilovic 2001). Indeed, misalignment of interests within an alliance (or domestic civil politics) can serve to weaken deterrence and provide opportunities for gray zone intervention.

Conflict initiators can similarly rely on proxies to complicate the deterrence calculus. Ambiguity regarding responsibility for an attack makes a retaliatory response less likely, especially if the target is looking for reasons not to retaliate (Borghard and Lonergan 2017). Recognizing the potential for agency problems, targets may discount the harm that proxies inflict. Reliance on third-parties may thus transform cases that would have been small wars into gray zone conflicts. The explicit delineation of an extended deterrence *quid pro quo* probably increases this risk, as red lines clarify what can be achieved in the gray zone.

# Russian Gray Zone Campaigns

We now test the plausibility of our argument about deterrence sensitivity by examining major Russian foreign interventions over the past two decades. Almost all cases feature cyber campaigns for disruption or influence. Some also feature intervention by special operations or conventional forces. Why does Russia bring more of its capabilities to some fights than others? We focus on Russia because its recent interventions, especially those featuring significant cyber operations, are often referenced as paradigmatic examples of gray zone conflict (Marten 2015; Driscoll and Maliniak 2016; Chivvis 2017). Specifically, we focus on four major Russian cyber campaigns targeting states that are geographically situated at different locations along the Western deterrence gradient: Estonia (2007), Georgia (2008), Ukraine (2014), and the United States (2016). The diversity of Russian targets provides an opportunity to conduct a natural controlled comparison of Russian choices under different deterrent circumstances.

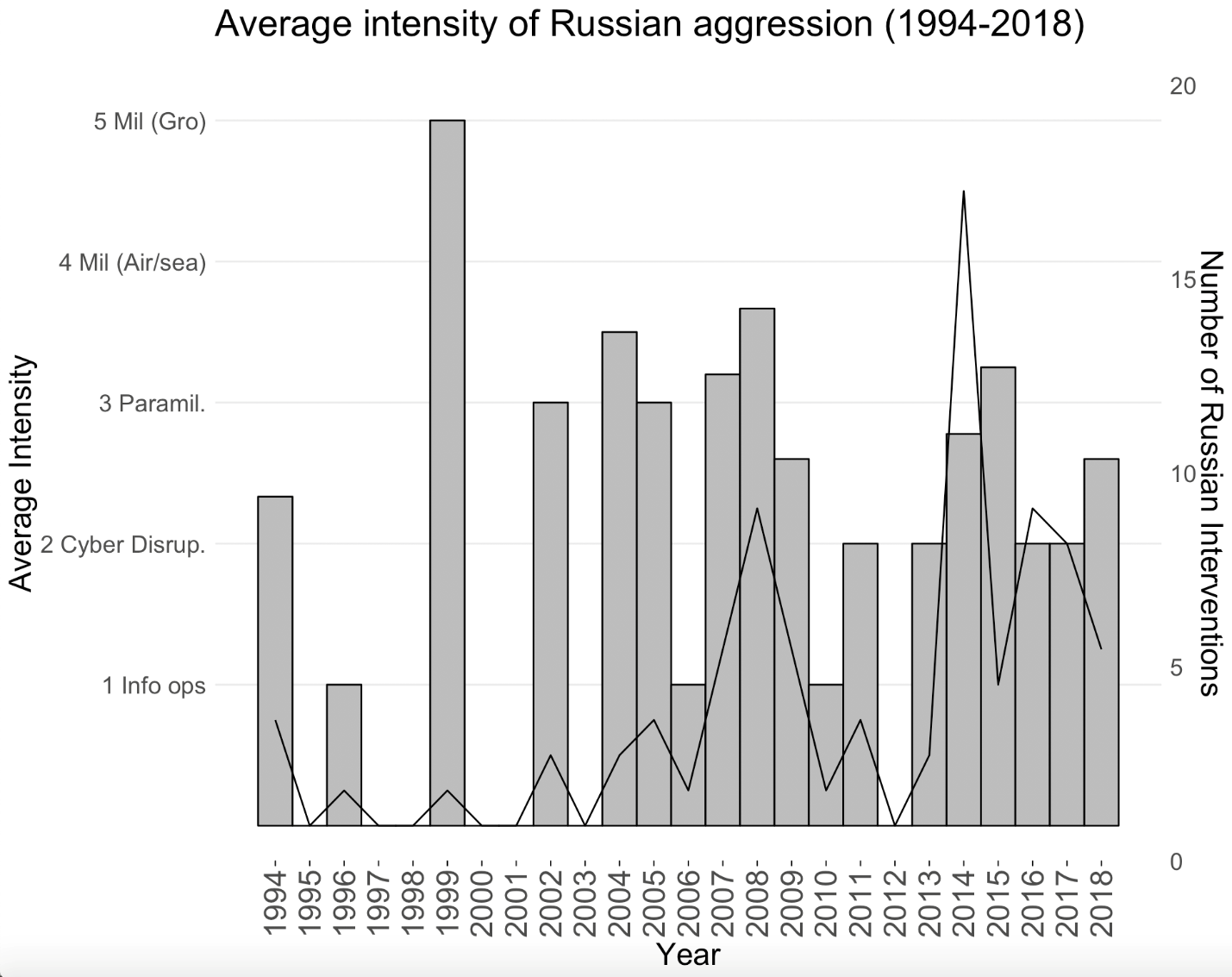
## Cross-National Data

It is perhaps fitting that data on Russian gray zone interventions are themselves ambiguous. Previous studies have compiled open source data on Russian-attributed cyber conflict over the past three decades. Two cross-national datasets – Dyadic Cyber Incident and Dispute (DCID) and Russian Electoral Interventions (REI) – cover almost entirely distinct samples (Valeriano and Maness 2014; Casey and Way 2017). Indeed, the only country-year that appears in both datasets is Ukraine 2014. 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. The different emphases of each dataset result in major coding heterogeneity.

We present an expanded and consolidated dataset of 82 cases of Russian intervention from 1994-2018. DCID and REI together describe 71 unique cases of Russian aggression that have either included some degree of cyber intervention or were cases of electoral interference.[[6]](#footnote-7) We have identified 10 additional instances of Russian cyber-attacks from 1994-2018 that are not covered in the previous datasets. Most of these new cases cover cyber conflict after 2011 (the latest year in DCID) that were non-electoral (the universe of cases in REI). We further include 3 cases of non-cyber Russian aggression from the International Crisis Behavior (ICB) dataset (Singer, Bremer, and Stuckey 1972). To resolve the heterogeneity across datasets, we compiled an entirely new coding of the intensity of Russian attacks. For each incident, we code whether Russia used conventional ground forces, conventional air or sea forces, paramilitary or covert forces, cyber disruption (service denial or industrial control system attacks), and information operations (social media and disinformation). By distinguishing between these five types of aggression, we obtain a clearer picture of the intensity of each case of Russian intervention.

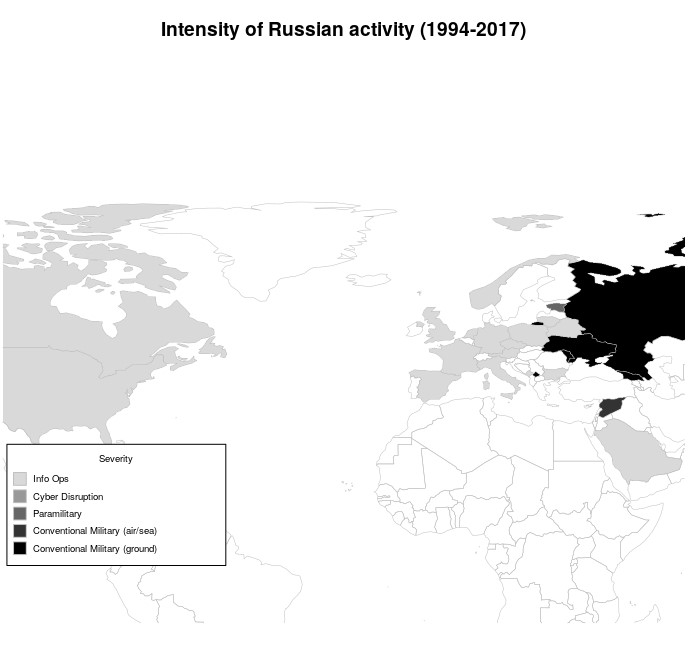
Figure 1 shows the frequency distribution of Russian gray zone operations since 1994. We follow the coding criteria used in DCID, coding each country-year’s intensity as the highest observed Russian intervention on a scale where information operations are the least intense type of intervention and ground troops are the most intense.[[7]](#footnote-8) Contrary to descriptions of gray zone conflict as new or the product of technological innovation, there does not appear to be an increase in low-intensity or non-kinetic Russian activity over time. Chechnya (1999) and Georgia (2008) represent the most intense Russian intervention and 2014 experienced the highest number of interventions (most of which were associated with Ukraine). Russian gray zone operations have not increased in intensity, but they do appear to be happening more frequently. This might reflect a weakening of Western deterrence, an emboldening of Russian leadership, or the maturation of technical capabilities. Whatever the cause, the result is likely to be a self-defeating (for Russia) strengthening of Western defenses and resolve given better information about the nature of the Russian threat. Like a stain on a microscope slide, Russian operations highlight the contours of the Western deterrence gradient.

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



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

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



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

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

## Major Cyber Campaigns

Russia is involved in numerous gray zone conflicts, but the actual shade of gray in each case depends on the deterrence gradient. For a more fine-grained test of our argument, we briefly examine the four major cyber campaigns attributed to Russia that feature prominently in the cybersecurity literature. The usual focus on cyber operations themselves tends to obscure the cross-domain and cross-national context of these operations. We employ a most similar case comparison by choosing cases that have the same conflict initiator (Russia) and the same means of low intensity conflict (cyber) but that differ in their geographical location and other military instruments employed (Bennett and Elman 2007). We code four rough categories of Russian operations in declining level of intensity, risk, and cost for the initiator (Russia): overt deployments of conventional military force, covert use of special operations or unattributed military forces, cyber operations that result in disruption of infrastructure, and information operations.

We do not focus here on the origins of Russian motives or their formulation in Russian foreign policy, even as understanding these is essential for devising practical policy responses in any given case. There are many potential explanations for Russian motives, to include the personality of Vladimir Putin, political competition for regime control, nationalist identity and status seeking, and geopolitical imperatives for security (Götz 2017). Rather we argue that how motives are expressed, whatever their origins, will be more or less constrained by Western deterrence. We will consider some counterarguments in the case narratives.

**Table 2**: Case comparison of Russian gray zone conflicts

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

Table 2 lists these cases by distance from Washington DC.[[8]](#footnote-9) Again the geographical pattern is striking. Moscow is more likely to pull its punches for cases closer to Washington. Russian operations directly against the United States have been limited to cyber influence and espionage operations. Operations against Estonia in 2007 were also restrained—Estonia is a NATO member—but further included a more punishing set 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 on Ukraine have been diverse and punishing but have fallen short of avowed military intervention. Georgia, by contrast, is not a NATO member and is deep in Russia’s sphere of influence. At the weakest end of the deterrence gradient, Russia intervened in Georgia in 2008 using not only cyber-attacks but also paramilitaries and overt military force.[[9]](#footnote-10) We will briefly consider each of them in chronological order.

### Estonia (2007)

Moscow coordinated a wave of DDoS attacks against Estonia following the relocation of a Soviet statue (Schmidt 2013). The gap in time between Estonia’s 2004 ascension to NATO and the 2007 Russian cyber campaign is telling. In Georgia and Ukraine, the mere prospect of future NATO membership (announced in the April 2008 Bucharest Summit Declaration) would provoke a Russian response. The Estonian attacks, by contrast, were a muted opportunistic protest, not a determined bid to change or return to the status quo. No one issued any clear demands or claimed responsibility, and Estonia did not replace the statue. The DDoS attacks were an ambiguous symbolic move calibrated to fall well below the threshold of a NATO response. The ambiguous legal status of a cyber-attack in 2007 both enabled and constrained Russia in this respect (Joubert 2012). NATO was highly unlikely to seriously consider formally responding so long as Russia avoided causing serious harm. Estonia’s defense minister considered but ultimately rejected invoking Article V, the collective defense clause of the NATO treaty, ultimately treating the episode as a domestic law enforcement matter (Traynor 2007). After the event, Tallinn became more resolved to bind with the West. Indeed, Estonia became a hub for coordinating NATO cyber defences. Because Russian moves were motivated by deterrence rather than efficiency, subsequent improvements in NATO cyber deterrence were not met by Russian escalation.

### Georgia (2008)

Georgia was hit by similar DDoS attacks amidst an even more fractious duel of competing narratives in online for a (Deibert, Rohozinski, and Crete-Nishihata 2012). Yet Russia also intervened militarily in South Ossetia and Abkhazia, an early example of cross-domain operations leveraging cyberspace. Russia’s intervention choices in this conflict, situated at the far end of the Western deterrence gradient, were relatively unconstrained. The same month as NATO announced a pathway to membership for Georgia, Russia announced that it would unilaterally increase peacekeepers in Abkhazia. Russia then used whatever mix of tools it needed to accomplish its objectives and did not pull its punches out of concern for Western counteraction. If anyone was deterred, it was NATO. As Driscoll and Maliniak point out, “because of Georgia’s location and its contested map, it is a security liability from the point of view of many in the West” (Driscoll and Maliniak 2016). 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 more forceful Western response would have only escalated the situation since Russia’s actions were chosen through a calculation that its objectives could be accomplished at reasonable cost.

### Ukraine (2014)

Can efficiency calculations alone explain the single-domain response in Estonia versus the multi-domain engagement in Georgia? One might argue that Russia values the stakes differently in each conflict and thus the geographical correlation observed in Table 2 is spurious. Indeed, 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 Georgian separatists since the early 1990s and was highly resolved to ward off Western encroachment. The Ukraine case, however, finds this alternative account wanting. The 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, and the Black Sea port of Sevastopol also makes Crimea more strategically relevant. If Russian moves were motivated by efficiency rather than deterrence, then we would expect more overt Russian military efforts in Ukraine, as in Georgia. On the contrary, despite Russia’s higher valuation of the stakes in Ukraine, we observe considerable restraint. Despite five years of protracted war—killing nearly ten thousand and displacing millions—so far there has occurred neither large-scale combined arms warfare nor unrestrained ethnic cleansing. Indeed, cumulative civilian deaths plateaued at about 4000 in 2015 (Driscoll and Steinert-Threlkeld 2019). The fact that the costs of war could be much higher, together with efforts made to allow both sides to save face, is suggestive of Russian motives for restraint.[[10]](#footnote-11)

Militating against the efficiency explanation, Russia took pains to create a fig leaf of ambiguity about the identity of Russian troops, the presence of Russian heavy weapons, and its role in orchestrating disinformation campaigns. Even though NATO has no formal commitment to Ukraine, conflict in a country that borders NATO allies like Poland and Hungary is implicitly shaped by Western deterrence. Russia would probably lose a conventional contest with NATO, risking nuclear escalation in the process. Russia acts circumspectly as a result. For example, when Malaysian Airlines flight MH17 was shot down over Donetsk by a Russian anti-aircraft system, Moscow withdrew its heavy weapons from the battlefield (Smith-Spark and Masters 2018). Russia has also not realized significant gain for all of its creative efforts in cyberspace (Baezner and Robin 2017). Endemic Russian cyber-attacks and information operations have had little impact on battlefield events (Kostyuk and Zhukov 2019). Even as social media manipulation is supposedly a Russian specialty, pro-Kremlin narratives have never really taken hold in Western Ukraine (Driscoll and Steinert-Threlkeld 2019). The cyber domain is especially attractive for a risk-averse opportunist, providing lots of ways to do something without doing too much. As Brantley et. al. points out, the modal diversity of conflict in Ukraine has lacked sufficient intensity to warrant outside intervention (Brantly, Cal, and Winkelstein 2017). Russia has the ability to impose its will on Ukraine, but it stops short. Russian moves in Ukraine are a second-best option shaped by Western deterrence.

### United States (2016)

A U.S. intelligence community statement released soon after the 2016 election 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” (Office of the Director of National Intelligence 2017). Moscow’s influence operations might thus be described as unrestrained, even brazen, and thus motivated entirely by efficiency calculations. Yet the choice to pursue this course of action in the first place was very much constrained by the implicit deterrence posture of the United States. Russia can safely assume that the most powerful military in the world will retaliate for armed attacks directly against its vital interests. While the United States had not designated its electoral processes “critical infrastructure” to explicitly signal that cyber interference against them might be proscribed, Russia still had to consider America’s power to retaliate. Russia sought opportunities to impose costs and seek benefits while minimizing the risk of retaliation, and it found them in covert manipulation of democratic discourse. Indeed, Russia's electoral interference has gone essentially unpunished by the United States to date, aside from the expulsion of some Russian intelligence officers and the application of some additional sanctions to an already heavy regime put in place after Ukraine. If Trump’s victory or subsequent policies can ever be credited to active measures by the Russian Federation, even in part, it would amount to one of the most consequential intelligence coups in history. It is just as likely that the Russian campaign simply added noise to one of the most chaotic campaigns in U.S. presidential history (Gelman and Azari 2017). Russian information operations were a low-cost gamble to influence an overdetermined outcome.

## Discussion

The overall pattern of recent Russian intervention is largely consistent with our hypothesis that deterrence encourages capable actors to engage in calculated restraint. As the deterrence gradient drops off from West to East, Russia has more freedom to pursue its international objectives. Geography does not determine deterrence, but it is correlated with other factors like military power, NATO membership, and the proximity of interests that shape deterrence credibility. While the degree of Russian interest does vary across these cases, the case of Ukraine demonstrates that Russia is sensitive to deterrence even when its interests are high. Differences in Russian choices also cannot be explained simply as an artefact of more options becoming available over time (i.e., maturation). The oldest cases (Estonia and Georgia) feature very different levels of intensity between them; as do the most recent (Ukraine and United States). To explain these differences, we must look to strategic incentives rather than technological capabilities. Gray zone conflict is not so much about the utilization of an expanding toolkit as careful decisions about what should be drawn from it.

# Every Silver Lining's Got a Touch of Gray

Gray zone conflict occurs when capable actors intentionally limit the intensity or capacity of aggression and refrain from escalation. It differs from other forms of irregular or asymmetric warfare that are also limited because one of the combatants simply lacks the means to escalate. Unlimited war for the guerrilla will be limited war for the state. Gray zone actors, by contrast, exercise calculated restraint out of concern for the potential consequences of aggression. 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. Limited conflict, ironically enough, is a symptom of deterrence success. Gray zone conflict, conversely, may be a reflection of weakness more than an expression of strength.

Just as there is a gray zone between war and peace, the distinction between effective and ineffective deterrence is also fuzzy. We have introduced the notion of the deterrence gradient, a straightforward extrapolation from the military loss of strength gradient, to describe credible deterrence as a continuous variable. Wherever deterrence is credible (due to a favorable balance of power, greater relative valuation of the stakes, costly signals of commitment, a reputation for resolve, etc.), revisionists will exercise considerable restraint as they probe to see what they can get away with. Wherever deterrence is not credible, revisionists will be more emboldened to use whatever means they have at their disposal to meet their objectives, limited only by efficiency concerns. The challenge lies in between these extremes, where the variable threshold of credibility creates a policy arena for limited conflict, and where it can be difficult to distinguish efficiency motivations from risk sensitivity. Doubling down on deterrence can mitigate conflict in the latter case but provoke escalation in the former.

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

This argument has implications for the debate over NATO expansion after the Cold War (Shifrinson 2016). When expansion is posed in starkly binary terms, expansion is seen as either a stabilizing force for Europe in the face of Russian recidivism or an irresponsible provocation of legitimate Russian security interests fuelled by liberal delusions (McFaul, Sestanovich, and Mearsheimer 2014; Mearsheimer 2014). If deterrence and conflict are continuous variables, however, then the real question is not simply whether NATO should or should not have expanded its security guarantees, but how far. One might thus argue that the first round of expansion to include the Eastern-Central countries (Poland, Hungary, Czech Republic) under the NATO umbrella helped to stabilize an historically conflict-prone part of Europe. After the fall of the Soviet Union and during a period of military and economic weakness, moreover, Russia was grudgingly willing to accept a downward revision of its European influence. One might also debate whether later rounds which brought in Baltic and Balkan countries made sense in whole or part. This is not the place to debate this history. We merely wish to point out that the alternative perspectives of NATO provocation and Russian aggression are better conceived as context specific variables rather than absolute qualities of either actor. The right question is not whether NATO should have expanded, but how far.

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

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

While Russian cyberattacks the focus of our empirical analysis, the theory should apply more broadly to all cases of gray zone conflict. Chinese incursions in the South China Sea offer another potential test. China’s use of “little blue men” suggests that Chinese opportunism and restraint are both enabling and constraining its foreign policy. That is, Beijing appears to fear that the use of more intense military operations risks provoking a Western response that both sides hope to avoid (Zhang 2019). Focusing on the credibility of deterrence rather than the novelty of means used for gray-zone conflict can also help to evaluate proper policy responses (Green et al. 2017). Confronted with gray zone provocations by capable actors like Russia, China, and Iran, the United States would be well advised to reinforce its strengths while avoiding overextension.

# References

Altman, Dan. 2018. “Advancing without Attacking: The Strategic Game around the Use of Force.” *Security Studies* 27 (1): 58–88. https://doi.org/10.1080/09636412.2017.1360074.

Angevine, Robert, Warden, John K., Russell Keller, and Clark Frye. 2019. “Learning Lessons from the Ukraine Conflict.” NS D-10367. Institute for Defense Analyses.

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

Bak, Daehee. 2018. “Alliance Proximity and Effectiveness of Extended Deterrence.” *International Interactions* 44 (1): 107–31. https://doi.org/10.1080/03050629.2017.1320995.

Bennett, Andrew, and Colin Elman. 2007. “Case Study Methods in the International Relations Subfield.” *Comparative Political Studies* 40 (2): 170–95. https://doi.org/10.1177/0010414006296346.

Borghard, Erica, and Shawn Lonergan. 2017. “The Logic of Coercion in Cyberspace.” *Security Studies* 26 (3): 452–81. https://doi.org/10.1080/09636412.2017.1306396.

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

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

Brantly, Aaron, Nerea Cal, and Devlin Winkelstein. 2017. “Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW.” Report. Army Cyber Institute. https://vtechworks.lib.vt.edu/handle/10919/81979.

Brodie, Bernard. 1957. “More About Limited War.” *World Politics* 10 (1): 112–22. https://doi.org/10.2307/2009228.

Brooks, Risa. 2008. *Shaping Strategy: The Civil-Military Politics of Strategic Assessment*. Princeton, NJ: Princeton University Press.

Carson, Austin. 2016. “Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War.” *International Organization* 70 (1): 103–31. https://doi.org/10.1017/S0020818315000284.

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

Carver, Michael. 1986. “Conventional Warfare in the Nuclear Age.” In *Makers of Modern Strategy from Machiavelli to the Nuclear Age.*, edited by Peter Paret, Gordon Craig, and Felix Gilbert, 779–814. New Jersey: Princeton University Press.

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

Chivvis, Christopher. 2017. “Hybrid War: Russian Contemporary Political Warfare.” *Bulletin of the Atomic Scientists* 73 (5): 316–21. https://doi.org/10.1080/00963402.2017.1362903.

Christensen, Thomas J., and Jack Snyder. 1990. “Chain Gangs and Passed Bucks: Predicting Alliance Patterns in Multipolarity.” *International Organization* 44 (02): 137–168. https://doi.org/10.1017/S0020818300035232.

Corbett, Julian. 1911. *Some Principles of Maritime Strategy*. Longmans, Green and Co.

Danilovic, Vesna. 2001. “The Sources of Threat Credibility in Extended Deterrence.” *Journal of Conflict Resolution* 45 (3): 341–69. https://doi.org/10.1177/0022002701045003005.

Deibert, Ronald, Rafal Rohozinski, and Masashi Crete-Nishihata. 2012. “Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War.” *Security Dialogue* 43 (1): 3–24. https://doi.org/10.1177/0967010611431079.

Driscoll, Jesse, and Daniel Maliniak. 2016. “With Friends Like These: Brinkmanship and Chain-Ganging in Russia’s Near Abroad.” *Security Studies* 25 (4): 585–607. https://doi.org/10.1080/09636412.2016.1220208.

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

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

Fallon, Michael. 2017. “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. https://www.gov.uk/government/speeches/rusi-landwarfare-conference.

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

Ganguly, Sumit. 1995. “Indo‐Pakistani Nuclear Issues and the Stability/Instability Paradox.” *Studies in Conflict & Terrorism* 18 (4): 325–34. https://doi.org/10.1080/10576109508435989.

Gartzke, Erik, and Jon R. Lindsay. 2015. “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace.” *Security Studies* 24 (2): 316–48. https://doi.org/10.1080/09636412.2015.1038188.

Gelman, Andrew, and Julia Azari. 2017. “19 Things We Learned from the 2016 Election.” *Statistics and Public Policy* 4 (1): 1–10. https://doi.org/10.1080/2330443X.2017.1356775.

George, Alexander, and Richard Smoke. 1989. “Deterrence and Foreign Policy.” *World Politics* 41 (2): 170–82. https://doi.org/10.2307/2010406.

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

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

Gordon, Michael R., and Bernard E. Trainor. 2007. *Cobra II: The Inside Story of the Invasion And Occupation of Iraq*. New York: Vintage Books.

Götz, Elias. 2017. “Putin, the State, and War: The Causes of Russia’s Near Abroad Assertion Revisited.” *International Studies Review* 19 (2): 228–53. https://doi.org/10.1093/isr/viw009.

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

Hammond, Grant T. 1990. “Low Intensity Conflict: War by Another Name.” *Small Wars & Insurgencies* 1 (3): 226–38. https://doi.org/10.1080/09592319008422957.

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

Hazelton, Jacqueline. 2017. “The ‘Hearts and Minds’ Fallacy: Violence, Coercion, and Success in Counterinsurgency Warfare.” *International Security* 42 (1): 80–113. https://doi.org/10.1162/ISEC\_a\_00283.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. 2019. “Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist.” *Journal of Strategic Studies* 42 (2): 212–34. https://doi.org/10.1080/01402390.2018.1559152.

Jervis, Robert. 1978. “Cooperation Under the Security Dilemma.” *World Politics* 30 (2): 167–214.

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

Johnson, Loch. 2013. “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. 2012. “Five Years after Estonia’s Cyber Attacks: Lessons Learned for NATO?” 76. Rome, Italy: NATO Defense College.

Kennan, George. 1948. “269. Policy Planning Staff Memorandum.” Records of the National Security Council NSC 10/2 RG 273. Washington: National Archives and Records Administration. http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm.

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

Kinross, Stuart. 2004. “Clausewitz and Low-Intensity Conflict.” *Journal of Strategic Studies* 27 (1): 35–58. https://doi.org/10.1080/0140239042000232765.

Kissinger, Henry. 1955. “Military Policy and Defense of the ‘Grey Areas.’” *Foreign Affairs* 33 (3): 416–28. https://doi.org/10.2307/20031108.

———. 1957. “Strategy and Organization.” *Foreign Affairs* 35 (3): 379–94. https://doi.org/10.2307/20031235.

Kornbluh, Peter, and Joy Hackel. 1986. “Low-Intensity Conflict Is It Live or Is It Memorex?” *NACLA Report on the Americas* 20 (3): 8–11. https://doi.org/10.1080/10714839.1986.11723411.

Kostyuk, Nadiya, and Yuri Zhukov. 2019. “Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?” *Journal of Conflict Resolution* 63 (2): 317–47. https://doi.org/10.1177/0022002717737138.

Lanoszka, Alexander. 2016. “Russian Hybrid Warfare and Extended Deterrence in Eastern Europe.” *International Affairs* 92 (1): 175–95. https://doi.org/10.1111/1468-2346.12509.

Lebow, Richard Ned. 2010. “The Past and Future of War.” *International Relations* 24 (3): 243–70. https://doi.org/10.1177/0047117810377277.

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

Lindsay, Jon R. 2013. “Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations.” *Journal of Strategic Studies* 36 (3): 422–53. https://doi.org/10.1080/01402390.2012.734252.

Lindsay, Jon R., and Erik Gartzke. 2018. “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.

Lindsay, Jon R., and Roger Petersen. 2012. “Varieties of Insurgency and Counterinsurgency in Iraq, 2003-2009.” Center for Irregular Warfare and Armed Groups Case Study Series. Newport, RI: Naval War College.

Marten, Kimberly. 2015. “Putin’s Choices: Explaining Russian Foreign Policy and Intervention in Ukraine.” *The Washington Quarterly* 38 (2): 189–204. https://doi.org/10.1080/0163660X.2015.1064717.

Matisek, Jahara W. 2017. “Shades of Gray Deterrence: Issues of Fighting in the Gray Zone.” *Journal of Strategic Security* 10 (3): 1–26.

Matláry, Janne Haaland. 2014. “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. https://doi.org/10.1057/9781137330307\_14.

Mazarr, Michael. 2015. “Mastering the Gray Zone: Understanding a Changing Era of Conflict.” Research Report. Strategic Studies Institute: US Army War College.

McFaul, Michael, Stephen Sestanovich, and John J. Mearsheimer. 2014. “Faulty Powers: Who Started the Ukraine Crisis?” *Foreign Affairs*, December 2014. http://www.foreignaffairs.com/articles/142260/michael-mcfaul-stephen-sestanovich-john-j-mearsheimer/faulty-powers.

Mearsheimer, John J. 2014. “Why the Ukraine Crisis Is the West’s Fault: The Liberal Delusions That Provoked Putin.” *Foreign Affairs*, October 2014. http://www.foreignaffairs.com/articles/141769/john-j-mearsheimer/why-the-ukraine-crisis-is-the-wests-fault.

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

Office of the Director of National Intelligence. 2017. “Assessing Russian Activities and Intentions in Recent US Elections.” Intelligence Community Assessment ICA 2017-01D. Washington, DC: National Intelligence Council. https://www.dni.gov/files/documents/ICA\_2017\_01.pdf.

Olson, William. 1990. “The Concept of Small Wars.” *Small Wars & Insurgencies* 1 (1): 39–46. https://doi.org/10.1080/09592319008422940.

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

Osgood, Robert. 1969. “The Reappraisal of Limited War.” *The Adelphi Papers* 9 (54): 41–54. https://doi.org/10.1080/05679326908448127.

Paul, Christopher, and Miriam Matthews. 2016. “The Russian ‘Firehose of Falsehood’ Propaganda Model: Why It Might Work and Options to Counter It.” Santa Monica, CA: Rand Corporation.

Pearlman, Wendy, and Boaz Atzili. 2018. *Triadic Coercion: Israel’s Targeting of States That Host Nonstate Actors*. New York: Columbia University Press.

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

Posen, Barry. 2003. “Command of the Commons: The Military Foundation of U.S. Hegemony.” *International Security* 28 (1): 5–46. https://doi.org/10.1162/016228803322427965.

Powell, Robert. 2015. “Nuclear Brinkmanship, Limited War, and Military Power.” *International Organization* 69 (3): 589–626. https://doi.org/10.1017/S0020818315000028.

Rauchhaus, Robert. 2009. “Evaluating the Nuclear Peace Hypothesis: A Quantitative Approach.” *Journal of Conflict Resolution* 53 (2): 258–77. https://doi.org/10.1177/0022002708330387.

Rid, Thomas. 2013. “Cyberwar and Peace.” *Foreign Affairs*, 2013. https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace.

Rovner, Joshua. 2011. *Fixing the Facts: National Security and the Politics of Intelligence*. Ithaca, NY: Cornell University Press.

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

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

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

Schneider, Jacquelyn. 2017. “The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict.” Dissertation, Washington, D.C.: George Washington University.

Schram, Peter. 2019. “Better Living Through Hassling: How to Prevent a Preventative War.” Working Paper.

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

Schweller, Randall L. 1996. “Neorealism’s Status‐quo Bias: What Security Dilemma?” *Security Studies* 5 (3): 90–121. https://doi.org/10.1080/09636419608429277.

Shifrinson, Joshua R. Itzkowitz. 2016. “Deal or No Deal? The End of the Cold War and the U.S. Offer to Limit NATO Expansion.” *International Security* 40 (4): 7–44. https://doi.org/10.1162/ISEC\_a\_00236.

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

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

Slayton, Rebecca. 2017. “What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.” *International Security* 41 (3): 72–109. https://doi.org/10.1162/ISEC\_a\_00267.

Smith-Spark, Laura, and James Masters. 2018. “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. 1965. “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.

Sobek, David, and Joe Clare. 2013. “Me, Myself, and Allies: Understanding the External Sources of Power.” *Journal of Peace Research* 50 (4): 469–78. https://doi.org/10.1177/0022343313484047.

Staniland, Paul. 2012. “States, Insurgents, and Wartime Political Orders.” *Perspectives on Politics* 10 (2): 243–64.

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

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

Traynor, Ian. 2007. “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. 2002. “Preface: Future Trends in Low Intensity Conflict.” *Low Intensity Conflict & Law Enforcement* 11 (2–3): 155–63. https://doi.org/10.1080/0966284042000279957.

Valeriano, Brandon, and Ryan Maness. 2014. “The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011.” *Journal of Peace Research* 51 (3): 347–60.

Votel, Joseph, Charles Cleveland, Charles Connett, and Will Irwin. 2016. “Unconventional Warfare in the Gray Zone.” *Joint Force Quarterly* 80 (January). http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80\_101-109\_Votel-et-al.pdf.

Wirtz, James J. 2017. “Life in the ‘Gray Zone’: Observations for Contemporary Strategists.” *Defense & Security Analysis* 33 (2): 106–14. https://doi.org/10.1080/14751798.2017.1310702.

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

Woodman, Stewart. 1991. “Defining Limited Conflict: A Case of Mistaken Identity.” *Small Wars & Insurgencies* 2 (3): 24–43. https://doi.org/10.1080/09592319108422992.

Zhang, Ketian. 2019. “Cautious Bully: Reputation, Resolve, and Beijing’s Use of Coercion in the South China Sea.” *International Security* 44 (1): 117–59. https://doi.org/10.1162/isec\_a\_00354.

# Appendix

This appendix provides supplemental information about the dataset of Russian gray zone campaigns introduced in the accompanying paper “After Deterrence: Explaining Conflict Short of War”

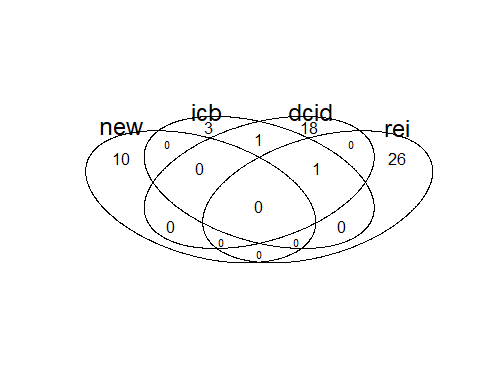
## Case selection

The universe of cases was created by first identifying cases of Russian foreign interventions from 3 prior datasets; ICB, DCID, and REI. Code replicating those findings is provided in the appropriate RMarkdown files. These cases were then supplemented with additional cases of Russian interference the authors were able to identify.

## Coverage of current datasets

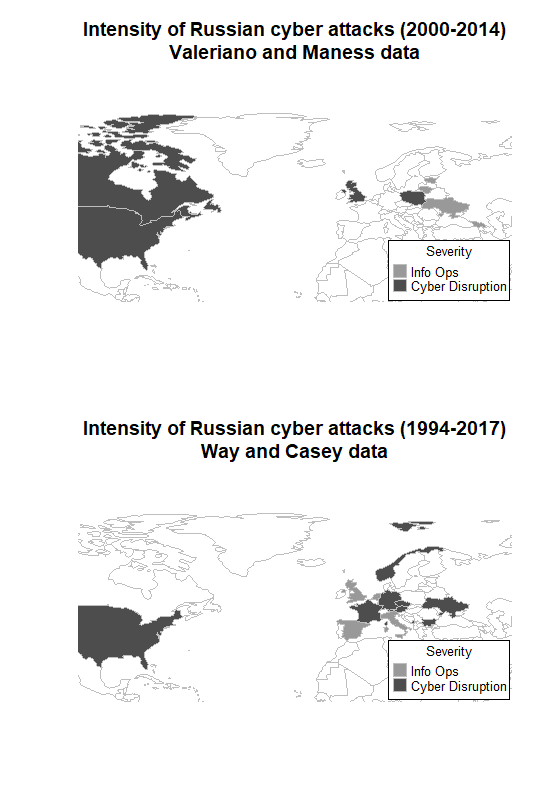
A comparison of what cases were covered in each individual dataset is provided here:

| **Target** | **Year** | **new** | **icb** | **dcid** | **rei** |
| --- | --- | --- | --- | --- | --- |
| Chechnya | 1994 | 1 | 0 | 0 | 0 |
| Belarus | 1994 | 0 | 0 | 0 | 1 |
| Ukraine | 1994 | 0 | 0 | 0 | 1 |
| Moldova | 1996 | 0 | 0 | 0 | 1 |
| Kosovo | 1999 | 1 | 0 | 0 | 0 |
| Georgia | 2002 | 0 | 1 | 0 | 0 |
| Ukraine | 2002 | 0 | 0 | 0 | 1 |
| Georgia | 2004 | 0 | 1 | 0 | 0 |
| Ukraine | 2004 | 0 | 0 | 0 | 1 |
| Lithuania | 2005 | 0 | 0 | 1 | 0 |
| Ukraine | 2005 | 0 | 0 | 1 | 0 |
| Moldova | 2005 | 0 | 0 | 0 | 1 |
| Belarus | 2006 | 0 | 0 | 0 | 1 |
| Estonia | 2007 | 0 | 0 | 1 | 0 |
| Georgia | 2007 | 0 | 0 | 1 | 0 |
| Georgia | 2008 | 0 | 1 | 1 | 0 |
| US | 2008 | 0 | 0 | 1 | 0 |
| Lithuania | 2008 | 0 | 0 | 1 | 0 |
| US | 2009 | 0 | 0 | 1 | 0 |
| Poland | 2009 | 0 | 0 | 1 | 0 |
| Ukraine | 2009 | 0 | 0 | 1 | 0 |
| Moldova | 2009 | 0 | 0 | 0 | 1 |
| Ukraine | 2010 | 0 | 0 | 0 | 1 |
| US | 2011 | 0 | 0 | 1 | 0 |
| Canada | 2011 | 0 | 0 | 1 | 0 |
| UK | 2011 | 0 | 0 | 1 | 0 |
| US | 2013 | 0 | 0 | 1 | 0 |
| Ukraine | 2013 | 0 | 0 | 1 | 0 |
| Ukraine | 2014 | 0 | 1 | 1 | 1 |
| US | 2014 | 0 | 0 | 1 | 0 |
| Canada | 2014 | 0 | 0 | 1 | 0 |
| UK | 2014 | 0 | 0 | 1 | 0 |
| Poland | 2014 | 0 | 0 | 1 | 0 |
| Moldova | 2014 | 0 | 0 | 0 | 1 |
| Ukraine | 2015 | 1 | 0 | 0 | 0 |
| Syria | 2015 | 0 | 1 | 0 | 0 |
| Germany | 2015 | 0 | 0 | 0 | 1 |
| United Kingdom | 2015 | 0 | 0 | 0 | 1 |
| Canada | 2016 | 1 | 0 | 0 | 0 |
| Austria | 2016 | 0 | 0 | 0 | 1 |
| Bulgaria | 2016 | 0 | 0 | 0 | 1 |
| Italy | 2016 | 0 | 0 | 0 | 1 |
| Montenegro | 2016 | 0 | 0 | 0 | 1 |
| Norway | 2016 | 0 | 0 | 0 | 1 |
| Netherlands | 2016 | 0 | 0 | 0 | 1 |
| United Kingdom | 2016 | 0 | 0 | 0 | 1 |
| United States | 2016 | 0 | 0 | 0 | 1 |
| United Kingdom | 2017 | 1 | 0 | 0 | 0 |
| Czech Republic | 2017 | 0 | 0 | 0 | 1 |
| France | 2017 | 0 | 0 | 0 | 1 |
| Germany | 2017 | 0 | 0 | 0 | 1 |
| Malta | 2017 | 0 | 0 | 0 | 1 |
| Netherlands | 2017 | 0 | 0 | 0 | 1 |
| Spain | 2017 | 0 | 0 | 0 | 1 |
| Netherlands | 2018 | 1 | 0 | 0 | 0 |
| Saudi Arabia | 2018 | 1 | 0 | 0 | 0 |
| Ukraine | 2018 | 1 | 0 | 0 | 0 |
| United Kingdom | 2018 | 1 | 0 | 0 | 0 |
| United States | 2018 | 1 | 0 | 0 | 0 |

The overlap between cases is seen here: 

## Consistency of current datasets

Aside from the cases covered, the intensity codings for current datasets are difficult to compare given their different scales. A more thorough analysis is provided in the appropriate R Markdown files, but a comparison of intensity codings in DCID (Valeriano and Maness) and REI (Way and Casey) is visualized here:



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. 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.

## Variable codings

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.

The following binary coding criteria were used for each case:

* resp\_infoops - Did Russia use information operations during this event? That includes propaganda, misinformation campaigns, etc
* resp\_cyberdisrup - Did Russia use cyber attacks during this operation? That includes hacking, phishing, cyber espionage, DDOS attacks, etc
* resp\_paramil - Did Russia use paramilitary troops during this event? Special forces, covert troops, speznatz, etc all count
* resp\_convmil\_airsea - Did Russia use conventional naval or air forces during this event?
* resp\_convmil\_gro - Did Russia use conventional ground troops like their army, artillery, tanks, etc during this event?

The complete dataset is provided in the appropriate .csv file. It includes sources used for the codings as well as justifications and explanations where needed.

1. NATO is not formally bound to assist Ukraine, but neither are they precluded from doing so. The issue for the Kremlin was ensuring that Brussels remained passive, and any measure that might help was worth taking. [↑](#footnote-ref-2)
2. Intelligence assessment and rational decision making, both defective in this case, are important for assessing the parameters of deterrence (Brooks 2008; Rovner 2011). [↑](#footnote-ref-3)
3. Conversely, as costliness of the Iraq war suggests, “gray zone” may be a poor description of cases where actors fail to exercise restraint because they do not understand their own deterrence sensitivities. [↑](#footnote-ref-4)
4. It is noteworthy that the United States relied on a regional partner (Israel) for the Stuxnet operation. [↑](#footnote-ref-5)
5. At least initially. For complications, see (Pearlman and Atzili 2018). [↑](#footnote-ref-6)
6. Our unit of analysis is country-year. See the data appendix for description of coding procedures, documentation of primary sources, and dataset comparison. [↑](#footnote-ref-7)
7. We code intensity as the highest level of intervention rather than the average since the types represent categorical, not ordinal variables. [↑](#footnote-ref-8)
8. 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)
9. Although not considered in detail here, Russian operations in outside cases like Kosovo and Chechnya are also consistent with the observed deterrence gradient. [↑](#footnote-ref-10)
10. Mixed messages of resolve and restraint are common in covert action (Carson 2018). [↑](#footnote-ref-11)