One if by land, and two if by sea: Cross-domain contests and the escalation of international crises

Anonymized author

May 25, 2021

Abstract

Speculation is growing that new domains of human endeavor and interaction have begun to trigger important changes in the nature of conflict. Technological advances have added cyber and space to more traditional domains of conflict (land, sea, air). Leading arguments, and anecdotes, suggest increasing competition across domains. Yet, empirical studies are largely constrained to single domains, limiting our collective ability to assess how domains interact. This study uses a new dataset of the domains in which states took military action during 412 international crises from 1918 to 2015 to test existing claims about cross-domain deterrence and cross-domain conflict. Far from being rare, these data show that cross-domain interactions are the modal form of conflict. Indeed, cross-domain conflict is no more frequent (proportionately) today than in decades past. Crises with cross-domain military interactions are also less violent and of no greater duration than crises involving belligerents using similar means.

Word count (excluding references) 8,730

1 Introduction

Increased technological sophistication has given rise to new modes of conflict as states have a growing number of "levers" or options through which to confront one another. These hostile interactions can take place symmetrically (like-for-like, within domain) or asymmetrically ("apples vs. oranges," across domain). Recent international crises in particular seem to demonstrate that asymmetric conflict is on the rise and may be a characteristic feature of a new era of conflict. Adversaries seem to be increasingly likely to respond to their opponent's military actions with dissimilar means. Hamas' cyber attacks in 2019 were met with Israeli airstrikes, Azerbaijani tanks clashed with Armenian drones in 2020 in the Nagorno-Karabakh region, Chinese malware attacks have recently joined the fray in an ongoing border skirmish with India, and Russian electoral inference in 2016 was met with the expulsion of Russian diplomats from the US and some sanctions rather than a military response due to concerns about the appropriateness of various kinetic and non-kinetic military operations. There is little consensus about whether to sound the alarm about dangerously escalatory cross-domain interactions or to caution against excess concern (Borghard and Schneider 2019). There also remains considerable ambiguity about whether recent cases of cross-domain conflict are emblematic of the future of warfare, or whether they are at most variations on a more durable set of themes (Gannon et al. 2021). As always with assessments of behavior, the question is "how new is new"?

While recent events have motivated a growing interest in understanding the settings in which states take military action and the consequences those choices have for international stability, the larger context of cross- or multi-domain conflict has not been studied systematically. Part of this is due to difficulty identifying military domains — is it simply geographic distinctions between land, air, and sea and their corresponding military commands? Where do new technologies like nuclear, space, and cyber fit into this typology? The second difficulty concerns limited empirical data concerning the conduct of conflict. While scholars have developed numerous detailed datasets of participants, duration, and outcome to understand conflict, empirically-oriented research concerning where contests take place, within which domain, has only recently received attention (Lindsay and Gartzke 2019a). Researchers and analysts typically frame their inquiries around particular emerging technologies (Sechser, Narang, and Talmadge 2019) or operations within individual domains, unable to address more formative questions about how domains interact (Allen and Martinez Machain 2017).

This paper takes an inductive, data-driven approach to identify spatial and temporal patterns in the military domains in which states operate during conflict as well as the relationship between cross-domain interactions and the intensity and duration of international crises. Rather than come up with a new typology of military domains, I take a commonly agreed upon understanding shared by practitioners and scholars that contains

the traditional domains of land, air, and sea as well as the recent domains of space, cyber, and weapons of mass destruction (WMD).[1] My motivation in gathering data on the conduct of conflict is driven by the recognition that the domains in which states fight are a reflection of actors' goals, resolve, and capability and subsequently shape important events like the severity and duration of conflict (Lindsay and Gartzke 2020). In doing so, I developed and introduce a novel dataset of the military domains in which 1,282 crisis actors operated during 425 international crises from 1918 to 2015. These data expand on the existing virtues of the familiar and well-regarded International Crisis Behavior dataset (Brecher and Wilkenfeld 2000).

Two initial findings contribute to existing research on the consequences of conflict domains. First, cross-domain conflict is prevalent, but not novel. Some degree of cross-domain military actions occur in 58% of crises over the past century, with 23% of crises involving completely dissimilar military actions by belligerents. Moreover that is not a recent phenomenon, as the rate of "cross-domainness" has remained more-or-less constant over the past century despite the accumulation of new military domains during that time period. The number of domains available does not itself seem to have triggered a greater reliance on cross-domain operations. Second, crises in which belligerents engage in cross-domain military conflict are less violent and no more durable than crises in which states respond with like-means. This evidence seems to support optimistic interpretations of the effects of cross-domain conflict and mitigate against the fears of some pessimists. While data on the more salient new domains like cyber remains limited at this time, insight about cross-domain interactions in more traditional military domains should inform theories of conflict deterrence and spiral as they are being developed to apply to more novel domains.

This paper proceeds in six parts. Section 2 identifies the existing state of the art concerning the domains in which states fight. Section 3 then identifies the theoretical basis underlying both the cross-domain pessimists and optimists, as applied to the intensity and duration of international crises. Section 4 provides an empirical test of these contrasting theories by introducing a novel dataset of the military domains in which states operated during international crises since 1918. Section 5 discusses the implications of these findings for theories of deterrence and the means of conflict, their application to contemporary foreign policy decisions, and avenues for future research. Section 6 concludes.

[1] While WMD is rarely a distinct military branch and has geographic overlap with the other domains, they do represent a distinct domain in how actors think about them in the international context. My concern here is less to get domains "right" and more to expose the diversity of options for conflict setting.

2 Existing theories of conflict escalation and how states fight

The vast array of theorized determinants of conflict escalation – defined here in terms of its intensity and scope – are primarily devoted to factors present before a contest occurs (Morgan 1994; Fearon 1995; Powell 1996). Since most wars end with some compromise rather than the total annihiliation of at least one of the warring sides, the actual conduct of conflict, its process, has much to tell us about when conflicts escalate (Wagner 2000) and how long they last (Slantchev 2004).

There is a well developed literature on how different *ways* conflicts are fought might influence conflict escalation. The ways in which militaries fight influences war's participants (Fordham 2004), victors (Rosen 1991; Lyall and Wilson 2009), severity (Talmadge 2019), and duration (Martinez Machain 2015) as well as what states are able to project power (Beasley 2015) and the balance of power (Glaser 1992). Despite interest in the means by which state engage in conflict, there is little agreement about how to conceptualize and categorize those means.

One broad framework for considering different means of conflict is in terms of the domains in which conflicts take place. There are many ways of thinking about domains, as they can be distinguished from one another by technology, tactic, geography, or purpose (Lindsay and Gartzke 2019a). Some have questioned the utility of conceptualizing these domains as distinct, especially as new domains like space and cyber increasingly play the role of supplementing rather than supplanting operations in the more traditional domains (Libicki 2012). Rather than engage in ontological debates about the best way to typologize conflict behavior, I take domains here as a useful starting point for thinking about differences in the ways that nations choose to fight, and how these differences affect observable attributes of conflict, such as duration or intensity. Practitioners think about these domains as distinct and these domains have known advantages and disadvantages (Lindsay and Gartzke 2019a). As already noted, I use the term "domain" here loosely to refer to land, air, sea, WMD, space, and cyber. Domains differ from one another in the constraints (and opportunities) they offer concerning power projection, movement, coordination, casualty risk, and cost – all factors that produce unique cross-domain dynamics regarding conflict intensity and duration (Lindsay and Gartzke 2020, 9–10).

If the problem of the security dilemma is to decide whether a particular response to an adversary's behavior will deter or escalate, the problem as applied to the conduct of conflict is whether the military means one chooses determine the likelihood of escalation. Snyder (1965, 187) described the importance of new (nuclear) means and escalation long ago. "[N]uclear 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". This view is widely credited with

originating discussion of the stability-instability paradox regarding the relationship between capabilities an actor possesses and the capabilities they use. The resulting debate created competing perspectives on escalation, characterized as deterrence and the spiral model. Snyder's deterrence perspective contrasts with the spiral model espoused by Jervis (1984). Powell (2015)'s recent work represents the newest attempt to theorize the relationship between power and risk. As the challenger uses more power to achieve its ends, its chance of winning increases, but so to does the risk of escalation. Although an important contribution to understanding conflict escalation and the deterrence and spiral models of conflict, existing theories of power and the risk of escalation leave what it means to bring "more power to bear" in a crisis unspecified (Powell 2015, 598).

Yet the amount of power is not synonymous with its type (Kreps and Schneider 2019). Just as the *quantity* of capabilities a state devotes to a contest influences its outcome, the *qualities* of those capabilities also matters (Carcelli and Gartzke 2017). One might plausibly claim that different military domains have different inherent level of belligerence. A nuclear strike is likely to be interpreted as a more intense form of military violence than a non-nuclear attack, even if the costs borne by the target are comparable in both cases (Tannenwald 1999). Yet this intuition remains coarsely formulated and may even prove empirically problematic, due to multi-causality, strategic interaction, and other factors. Foundational escalation metaphors, such as "ladders" (Kahn 2007) often parallel the distinction of domains, making separating out cause and coincidence more difficult. Libicki (2009, 28–29), for example, notes that belligerence increases as an actor shifts from diplomatic and economic aggression to cyber, then physical force, then nuclear force. But whether such patterns are more indicative of the effects of the form of competition or of the intentions of competitors remains unclear. Nor is the belligerence of each domain conceptually strategically, as the domains in this the opponent is operating are left out of the equation. Escalation may or may not be associated with whether responses are symmetric or asymmetric. Whether the move from one "physical force" domain to another is consistent with the deterrence or spiral model of conflict remains to be shown.

With these issues in mind, evaluations of the importance of actions in domains has recently shifted to theorizing about interactions across domains (Lindsay and Gartzke 2019b). There is suspicion that cross-domain interactions are more prevalent now because there are more (and newer) domains in which states can operate. While study on conventional-nuclear interactions is no longer in its infancy (Kissinger 1960; Carver 1986), this has recently expanded to cross-domain interactions involving space (Early 2014; Lin-Greenberg and Milonopoulos 2021) and cyber (Schneider 2017; Lindsay and Gartzke 2018; Kostyuk and Zhukov 2019). Both researchers and policymakers have expressed concern that these and other new tools of warfare may strengthen or embolden revisionist forces in world affairs (Brands 2016), although skepticism about the

novelty and efficacy of these "new" forms of warfare has also cast some doubt on those concerns (Gannon et al. 2021).

Empirical evidence, however, remains limited due in large part to the very novelty and putative heterogeneity of these emerging domains (Horowitz 2020). Even where recent empirical research has made headway in identifying the ownership and use of new modes of warfare, the efforts are contained to a single capability or domain. As a result, existing research on cross-domain conflict tends to approach the "cross" component of the subject in terms of within-actor behavior, rather than across actors. As Nye (2017, 46) notes, "it is a mistake to see the cyber realm in isolation. The term "cyber deterrence" can be confusing because theorists tend to focus on in-kind or in-domain deterrence rather than on a broad range of tools that can be used both actively and passively and with graduated effects. A response to a cyberattack need not be by cyber means any more than a response to a land attack need be by the army rather than naval or air forces."

3 The Dialectic Across Domains

"A ship's a fool to fight a fort."[2] But is it wiser for a commander, or a nation, to attack a fort with a fort? Interpreting "foolish" actions as those that increase a conflict's violence and/or duration, perhaps unnecessarily, I identify two sets of disparate expectations about cross-domain interactions. Despite the contrasting predictions in the literature best characterized by the classical dialectical debate between deterrence theory and the spiral model, both perspectives share the assumption that the manner in which states engage in a crisis influences whether it is resolved peacefully or violently (Kydd 1997; Zagare and Kilgour 1998). For the spiral model, the threat of punishment backfires and causes one's opponent to escalate while for the deterrence model, the threat of punishment elicits compliance (Jervis 1976). These perspectives thus differ in whether demonstrations of resolve and/or capability succeed or fail when they involve transporting actions to a military domain in which one's opponent is not operating.

3.1 Cross-domain escalation: the danger of taking an ear for an eye

Crises in which actors interact in dissimilar military domains may be more violent and/or last longer because cross-domain interactions complicate interpretations of proportionality and the scope of disputed stakes, thus contributing to misinterpretation of resolve (Morrow 2019). If a belligerent taking action with 100 ground troops is met with a defender deploying 200 ground troops, the belligerent could reasonable interpret the defender's action as a "raise" indicating the defender places a high value on the issue(s) in dispute. But if the defender responds to a deployment of 100 troops with 5 aircraft, it is less clear whether that is a

[2]The quote is generally (mis)credited to Admiral Lord Horatio Nelson, RN (Ferreiro 2016).

raise, or instead is an effort to achieve something different, such as saving face. Cross-domain conflict thus presents actors with an apples to oranges comparison, making it more difficult to assess relative resolve or an opponent's value for the issue(s) at stake. This injection of (additional) ambiguity could make a negotiated settlement more difficult by clouding evaluations of the bargaining range.

Uncertainty can cause, or worsen, a contest by creating incompatible expectations about a contest's likely outcome or utility (Fearon 1995; Gartzke 1999). Asymmetry in the military domains in which belligerents are taking actions can be a source of that uncertainty. Cross-domain interactions may be perceived by the adversary as shifting to a domain where one has escalation dominance because you highly value the stakes of the conflict. Since each military domains has different strengths and weaknesses concerning outcomes like credibility, costs, signaling, and relative war fighting ability, operating in a different domain that your adversary may signal a difference in one's tolerance for cost and risk (Gartzke et al. 2017). One can represent this aspect of military domains in terms of a game of rock, paper, scissors, where each domain's characteristics bring advantages against some of your opponent's chosen domains, but disadvantages against others (Lindsay and Gartzke 2019a, 16). In discussing the dangers of Chinese power projection from land, former US National Security Adviser H.R. McMaster (2016) advised practitioners recognize the synergy "between joint force capabilities and how, you know, really joint operations - it's rock, paper, scissors, you know? So if you can - if you have all of those tools available - maritime, aerospace, cyberspace, land capabilities - then you're able to pose that enemy with multiple dilemmas."

While presenting your enemy with multiple dilemmas — responding to your adversaries "rock" with "paper" — may help you win the conflict, it could also produce an incentive for your opponent to do the same — respond again with "scissors" — thus encouraging escalation. Responding in-kind — playing rock against rock — may be de-escalatory because it represents a symbolic gesture to opt against one's most efficient response (paper), since doing do would require the opposing side to engage in a new, even more efficient response (scissors) (Biddle and Oelrich 2016). By responding in-kind, states can agree to call it a draw in a way that represents an explicit or tactic compromise (Carson 2016). Conversely, engaging in a new military domain may unintentionally create an "escalatory updraft" if the opponent misinterprets what should be a tit-for-tat response that ends aggression with one that instead escalates it (O'Neill 1991, 104). To return to Powell (2015)'s logic about bringing more power to bear, taking action in a new domain may help one side secure victory by represent a reduction in cost, but the very logic of escalation dominance that generates that outcome also means interacting in the new domain represents an increase in cost for your opponent, with adverse consequences for the likelihood of a peaceful settlement. Cheap and easy can be attractive, but it sends mixed messages. An opponent may be cowed by superior capabilities across domains, but they may

also be encouraged by limited evidence of an opponent's willingness to pay the high price of a larger contest.

Pessimist Hypothesis 1: *Interstate crises in which belligerents act in dissimilar military domains should be more violent than those in which belligerents act in similar military domains.*

Pessimist Hypothesis 2: *Interstate crises in which belligerents act in dissimilar military domains should be longer in duration than those in which belligerents act in similar military domains.*

States often share an assumption that opponents will "follow precedent by responding in kind with similar weapons against a similar target set", so failing to do so risks un-calibrated escalation (Warden 2018, 24). Scholars have raised this concern in the US-China context in arguing "war at sea could thus quickly become a war on land, potentially even raising risks of nuclear escalation if the US starts to erode potential capabilities relevant to China's nuclear arsenal" (Talmadge 2019, 880–81). In the cyber context, scholars have argued retaliating to physical force with a cyber attack may raise issues of proportionality (Libicki 2009). While China thinks that cyber attacks are a proportional response to US trade pressure given the stakes each place on the sectors being harmed by the other actions, the United States disagrees. "The U.S. approach to Chinese gray zone tactics seems to be consistently several steps behind the threat. As in the Russia case, this is likely due in large part to the absence of a coherent strategic approach, leading to ad hoc U.S. responses from one crisis point or domain of interaction to the next." (Hicks and Friend 2019, 8).

3.2 Cross-domain deterrence: the safety of playing chess while your opponent is playing checkers

Just as deterrence and the spiral model make contrasting claims from similar priors, the opposite (optimist) logic could also be at play in assessing cross-domain escalation. Crises involving states taking military actions in dissimilar domains could be less likely to escalate by communicating a change in the stakes and a willingness to escalate or by giving one side the upper hand if conflict actually breaks out (Rovner 2020). The apples to oranges analogy may be backwards; rather than creating confusion about resolve and the opponent's evaluation of the stakes, a willingness to play a different game entirely may sharpen that logic in a way that signals it may be better to try to resolve the conflict without fighting. The discriminability of moving to a new domain is a way for an actor to simultaneously signal resolve and restraint in a way that reduces the intensity and duration of a conflict logically similar to coordinating focal points as seen with covert operations (Carson 2016).

Rather than simply thinking of military domains as playing rock, paper, or scissors, the different virtues of various domains also creates distinctions in what it means to "play" one of them. Threats differ from forward

deployments which are further different from seizing territory or discharging a rocket (Lai 2004). In this way, operating in a new domain could deter rather than inflame by providing an avenue to graduated escalation (Cashman and Robinson 2007). Reinforcing an army unit by putting bombers on alert or forward deploying a naval unit could be a graduated way of signaling resolve and a willingness to escalate without necessarily increasing the number of army troops already on the battlefield (Slantchev 2005). Using the same assumption of escalation dominance, action in a new domain in which your opponent is not operating because they do not have escalation dominance in that domain can be a costly signal that makes a negotiated settlement more likely (Cimbala 1994; Quek 2013). In the same way that children on a playground may yell 'hotter' or 'colder' as their blindfolded classmate tries to find some object, operating in new domains can add credibility to verbal statements about whether an actor perceived an offered negotiation as preferable to continuing to fight. Furthermore, deterrence may work not because of mutual vulnerability, but because of one-sided fear about overwhelming punishment (Green 2020; Lieber and Press 2020). If operating in a new domain during a crisis is indicative of a state's willingness to take action in a domain where they have escalation dominance, that may convey to the other side that the state is willing to incur a higher cost and they are thus better off backing down.

Optimist Hypothesis 1: *Interstate crises in which belligerents act in dissimilar military domains should be less violent than those in which belligerents act in similar military domains.*

Optimist Hypothesis 2: *Interstate crises in which belligerents act in dissimilar military domains should be shorter in duration than those in which belligerents act in similar military domains.*

Historically, Nixon placing bombers on nuclear alert during the 1969 Giant Lance operation demonstrated the introduction of a new domain as a way to signal a willingness to gradually escalate or de-escalate based on their opponent's actions (Sagan and Suri 2003; Burr 2005). This case is consistent with existing theories of signaling in finding that some domains are better suited to turning the dial incrementally rather than all at once (Post 2019; Montgomery 2020). President Kennedy had a similar rationale behind the "flexible response" doctrine in 1961, which aimed to provide more options for controlled escalation. In the event of more limited Soviet aggression like an attempt to hold Berlin hostage, proponents of flexible response hoped the more credible threat of responding with other conventional forces would be sufficient to get the Soviet Union to back down (Duffield 1991).[3] Similarly, a ceasefire was declared between Israel and Hamas the day after Israel responded to Hamas' cyberattacks with an airstrike (Morris, Eglash, and Balousha 2019). One way to interpret this event is the very conditions that make a cross-domain response a threat of immediate

[3]There is disagreement concerning whether Kennedy actually believed in — and would have implemented — "flexible response" or whether it was political theater (Gavin 2001). I use this example simply to illustrate the strategic logic held by proponents of the policy.

escalation make it conducive to medium and long-term de-escalation. By showing that an opponent has crossed a red line in the intensity of their aggression, an unexpected cross-domain response could convey that there are significant costs to be had if they do not pull back (Altman 2018).

As an aside, cross-domain interactions may not be the direct cause of escalation (or de-escalation), but rather an observable indicator for different motives to escalate in a way that masks the stakes (Slantchev 2011). States with more at stake may be more willing to escalate, but cross-domain interactions may communicate that poorly since it relies on your opponent identifying the costs of your action when that same action would generate different costs for them (Dafoe, Renshon, and Huth 2014; Renshon 2016; Lupton 2018.) Rather than try to empirically identify whether the underlying causes of cross-domain interactions are directly or indirectly determinants of conflict intensity, I simply hope to shed light on the association between the use of these domains — whatever their origins — and crisis outcomes.

4 Empirics

4.1 Research Design

The study's primary empirical contribution is a new dataset detailing the domains in which military actions or conflict occurred during 425 distinct crises from 1918 to 2015. In sum, the new data contains information on 1,282 crisis actors, the majority of which are states.[4] This crisis-domain dataset represents – to the best of my knowledge – the most extensive data collection available on the domains in which militaries operate during conflict.

Doing so involved three distinct steps. First, a research team event coded the 425 crises in the International Crisis Behavior (ICB) dataset, identifying the military domains in which crisis actors acted. Second, I re-organized that data to the crisis-dyad level using pre-existing work on ICB crisis-dyads as well as new coding for crisis-dyads post-2010 – the most recent year coded in pre-existing efforts. Third, I create a new measure of the dissimilarity of the domains in which each side in the crisis took military actions, a numeric measure that I refer to as "cross-domainness". I discuss these steps in greater detail below.

4.1.1 Event coding

A research team extended the ICB dataset by gathering extensive data on how actors interacted during crises. A crisis is defined as an international event where 1) an actor perceives a threat to one or more of its

[4]International organizations and non-state actors sometimes deploy military or quasi-military capabilities like peacekeepers or foreign aid distributors. I do not consider the military logic of these actors here, but the data is available for future work.

basic values, 2) there is a finite timeline for responsing, and 3) there is a heightened probability of military hostilities (Brecher and Wilkenfeld 2000). A crisis can escalate to an actual military dispute, but that does not always happen. This provides variation in the dependent variable since I can compare cases where a crisis did violently escalate to cases where the crisis did not. The dataset introduced here contains detailed information on the military domains used by each actor during every international crises. As such, the unit of analysis is the crisis-actor and the newly coded variables are binary values representing whether that actor took military action in a given domain during the crisis.

The data source used by the coders was the ICB crisis narratives that provide qualitative descriptions of each crisis. Unlike other event datasets that pool from multiple news sources with various data generating processes, the ICB narratives are written in a systematic fashion, contain comparable levels of detail, and were written by the same research team at the University of Maryland. This reduces concerns that variation among crisis variables is due to variation in the measurement process. For example, more recent crises do not have more detailed crisis narratives which is not the case for the reporting of militarized interstate disputes captured by scraping news sources. The ICB narratives are also accompanied by the widely-used and well-regarded ICB dataset, allowing the newly coded domain variables to be integrated into the broader ICB data project.

The data created here involves the domains in which states took actions during international crises.[5] I define the domains in which a crisis-actor can take a military action based on the military units that undertook the action, as described in Table 1. The coders distinguished actions, speech acts, and thoughts for consistency with pre-existing event datasets like CAMEO and Phoenix (Schrodt et al. 2005; Althaus et al. 2020). Actions are defined as physical acts performed by one of more actors. Examples of military actions include raises in alert level, mobilizations, fortification, military exercises, weapons tests, deployments, shows of force, blockades, border violations, attacks, invasions, and bombardments. Planning to take an action does not constitute an action unless this action is subsequently carried out. For example, a state making a verbal threat to send tanks into a neighboring country is not coded as a ground action unless the state deployed, attacked, or otherwise took a subsequent physical action with land units.

For each crisis, two research assistants coded the events that occurred sentence by sentence as a series of actions undertaken by an actor along with supporting details like when the action took place, where, and to what effect. The domain codings were then double checked, with particular attention paid to the less common domains of WMD, space, and cyber. The final version of the data includes an aggregation of the

[5]This is a subset of a broader project producing event data using the ICB narratives. For the complete event data and more detailed explanation of the underlying ontology, see Carcelli et al. (2021).

Domain	Description
Air	Bombers, fighters, and missiles
Cyber	Information operations and cyber disruption
Land	Armored vehicles, artillery, and troops
Sea	Aircraft carriers, submarines, and surface ships
Space	Satellites and surveillance beyond the earth's atmosphere
WMD	Nuclear, chemical, and biological weapons

Table 1: Military domains coded for each crisis actor. Codings are binary with 1 indicating the actor took an action in that domain during the crisis and 0 otherwise.

multiple different codings that exist for each case. Figure 1 shows the distribution of actions taken in each domain by each crisis actor. Consistent with expectations, the past century witnessed crisis-actors most often operating in the land domain, with significantly fewer WMD, cyber, and space actions taking place. Even so, the prevalence of WMD events may appear higher than expected. This is because the domain variables refer to where the action took place, rather than what was used during the action. As a result actions like raising nuclear alert levels or forward deploying nuclear bombers constitute WMD "actions" even if nuclear bombs were not subsequently detonated. The low number of space and cyber actions do not reflect the rarity of military action in the space and cyber domains, but rather the rarity of those domains *in international crises*. This distinction is important, as existing work has documented numerous cases of cyber attacks that occur outside the universe of international crises defined by the International Crisis Behavior project (Valeriano and Maness 2014).

Of course, actors do not always contain their military activities to a single domain. Conventional wisdom surrounding the efficacy of full-spectrum military forces rightly leads to the suspicion that actors often engage in multiple military domains simultaneously, especially as the stakes of a conflict heighten. Figure 2 describes the combination of military domains that each crisis-actor undertook. While the sole deployment of land forces still remains by far the most common form of military action, combined land- and air operations is the second most common, followed by land, sea, and air being used in unison.

4.1.2 Identifying crisis-dyads

The original ICB data exists at two levels of analysis, the crisis-level and the crisis-actor level. While the actor-level data latter contains more granularity, it leaves the role of each actor unspecified. So after identifying the military domains in which crisis-actors took actions, this new data was merged with existing data on ICB crisis-dyads (Hewitt 2003; Beardsley and Asal 2009; Levin-Banchik 2020). An ICB crisis-dyad is an ICB crisis in which both sides are sovereign states, at least one state meets the original three ICB crisis conditions, and at least one actor perceives that the other has directed a threat or hostile threat against it.

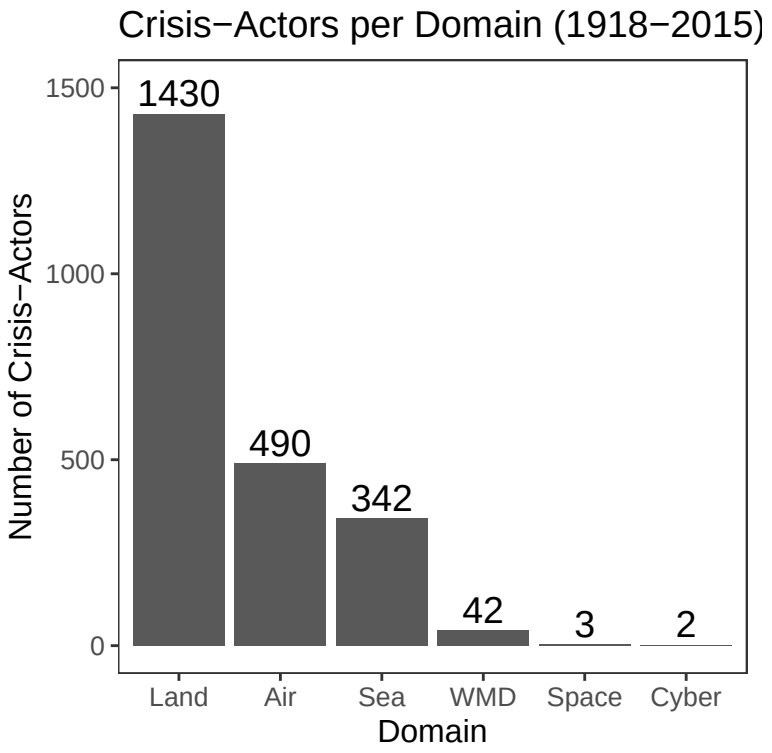

Figure 1: Distribution of domains by crisis-actor

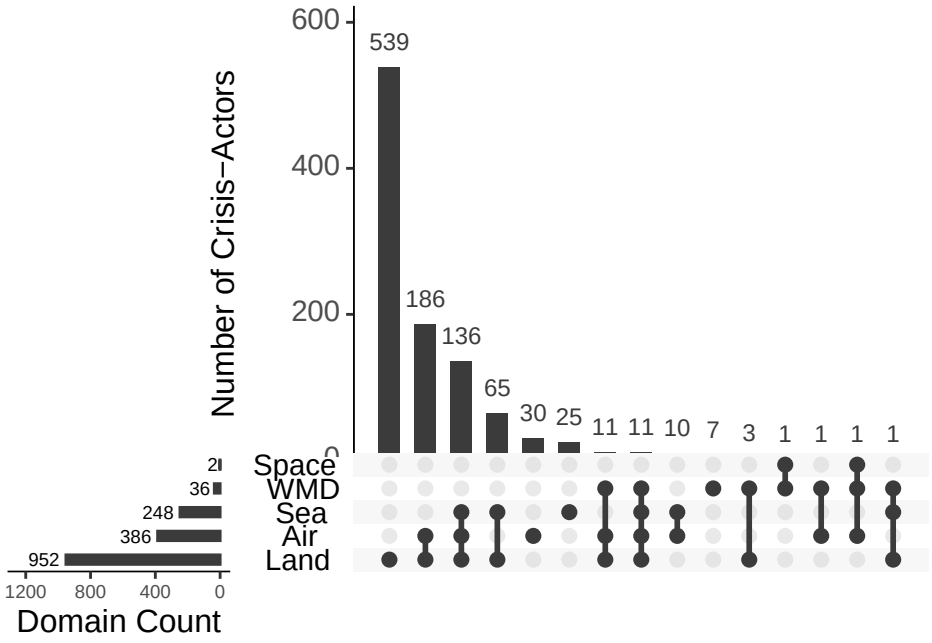

Figure 2: Combination of domains for each crisis actor. Each bar represents the number of crises with that unique intersection of domain values present

The pre-existing crisis-dyad data ends at 2010, so new coding of crisis-dyads was done on the post-2010 crises.

The coding followed the same rules and procedures outlined by Hewitt (2003). The end result is actor-level

dyad information for 425 ICB crises.

Numerous crises involve multiple dyads if, for example, military coalitions were involved. To simplify coding, when multiple actors participated on the same side in the conflict, that side was coded as having taken actions in a given military domains if any actor on that side took actions in that domain. For example, if both France and the United States were coded as side A in a crisis and France deployed naval assets and the United States deployed ground forces, side A is simply coded as having taken action in both the naval and land domains.

4.1.3 Measuring cross-domainness

The third and final step involves identifying the dissimilarity of the domains in which each side of each crisis-dyad took actions. I call this measure "cross-domainness", which is a variable at the crisis level of analysis bounded between 0 and 1. For each crisis, if the two sides took actions in identical domains, cross-domainess is low. If the two sides took actions in entirely distinct domains, cross-domainness is high.

I produce this measuring by using a Jaccard similarity coefficient to compare the military domains in which each side in a crisis-dyad operated. This measure identifies the union of domains in which each side took actions as a ratio of those in which only one side took action, such that for a crisis-dyad with two sides A and B, $J_{(A,B)} = \frac{A \cap B}{A+B-(A \cap B)}$. Table 2 provides descriptive examples of how domain similarity in various crises is measured. During North Korea's nuclear test in 2009, North Korea launched a satellite followed by an underground nuclear test. The United States, Japan, and South Korea mobilized naval forces as a part of military drills and kept interceptor-capable ships in the region following those drills. Since North Korea (side A) took action in the space and WMD domain while the US, South Korea, and Japan (side B) responded in the naval domain, this crisis had an entirely cross-domain interaction – the two sides took no military action in the same domain. By contrast, the 1965 Kashmir crisis involving India, Pakistan, and China only involved land forces being deployed. India (side A) sent troops across the ceasefire line in response to infiltration by Pakistani "freedom fighters" (side B). China (also side B) then responded with troop movements near the border. In this case, the two sides responded exclusively "in-kind", so this crisis was entirely within-domain.

The Jaccard measure is appropriate because each crisis contains precisely two sides (two vectors to compare), the values are binary, and I am concerned with the similarity of measures that were employed as opposed to those that were not. Similar measures like the simple matching coefficient (SMC) are less appropriate since there is variation across space and time about what 0's mean. In some cases, 0's are an omission by choice (states chose not to act in this domain) but in others they represent omission by necessity (states lacked the capacity to act in this domain). Although neither the US nor Vietnam used WMDs during the Vietnam war, that doesn't make their military strategy similar because the US could have done so but did

Crisis	Belligerents	Land	Air	Sea	WMD	Space	Cyber	Jaccard
N Korea Nuclear IV (2009)	US, Japan, S Korea	-	-	1	-	-	-	1
	N Korea	-	-	-	1	1	-	
Yemen War IV (1967)	Yemen, Egypt	1	1	-	1	-	-	0.67
	Saudi Arabia	1	-	-	-	-	-	
Kashmir I (1947)	India	1	1	-	-	-	-	0.5
	Pakistan	1	-	-	-	-	-	
Gulf of Tonkin (1964)	S. Vietnam, U.S.	1	1	1	-	-	-	0.33
	N. Vietnam	1	-	1	-	-	-	
Kashmir II (1965)	India	1	-	-	-	-	-	0
	Pakistan, China	1	-	-	-	-	-	

Table 2: Example of cross-domainness measure at the crisis-level using the Jaccard similarity coefficient. The measure is bounded between 0 and 1, with 0 indicating the two sides took actions in identical domains and 1 meaning complete dissimilarity.

not, while Vietnam could not have. Thus, 0's mean different things. I avoid this problem by measuring similarity in terms of what they did use, in which domain.[6] This measurement also appropriately tests the theories presented here since they concern the consequences of states interacting in unlike means. Similar concepts like the number of domains in which actors take military action are important, but are not the criteria of interest here since this paper is not investigating whether full-spectrum conflicts are more violent or longer than single-domain conflicts.

Figure 3 represents the distribution of cross-domainness for all ICB crises. This figure demonstrates that cross-domain military crises are not unusual, just the opposite. Some amount of cross-domain conflict behavior represents the modal form of crisis interaction over the past century. Of the 425 ICB crises, 23% are entirely cross-domain, meaning the two side had zero overlap in what military domains they operated in during the crisis, and 58% had at least some amount of cross-domain interaction. In only 42% did both sides behave in-kind. Figure 4 shows that the temporal trend of cross-domain interactions runs contrary to conventional wisdom. Despite the common demarcation of the nuclear age and advent of new domains like cyber and space, cross-domain conflict is not an emerging property of new, technological conflict domains (at least not within crises). Although new military tools have become available to states at an arguably ever greater pace, they have not led to an increase in cross-domain activities. Either these domains are not being utilized in international crises, or they are being utilized in about the same way that older domains of conflict were and continue to be exercised. There is no evidence in these data of a transformation of military affairs related to cross-domain conflict. Rather, cross-domain conflict has been, and continues to be, a common feature of conflict behavior generally, at least within crises.

[6]For an overview comparing different similarity measures and criteria for their appropriate application, see Egghe (2010).

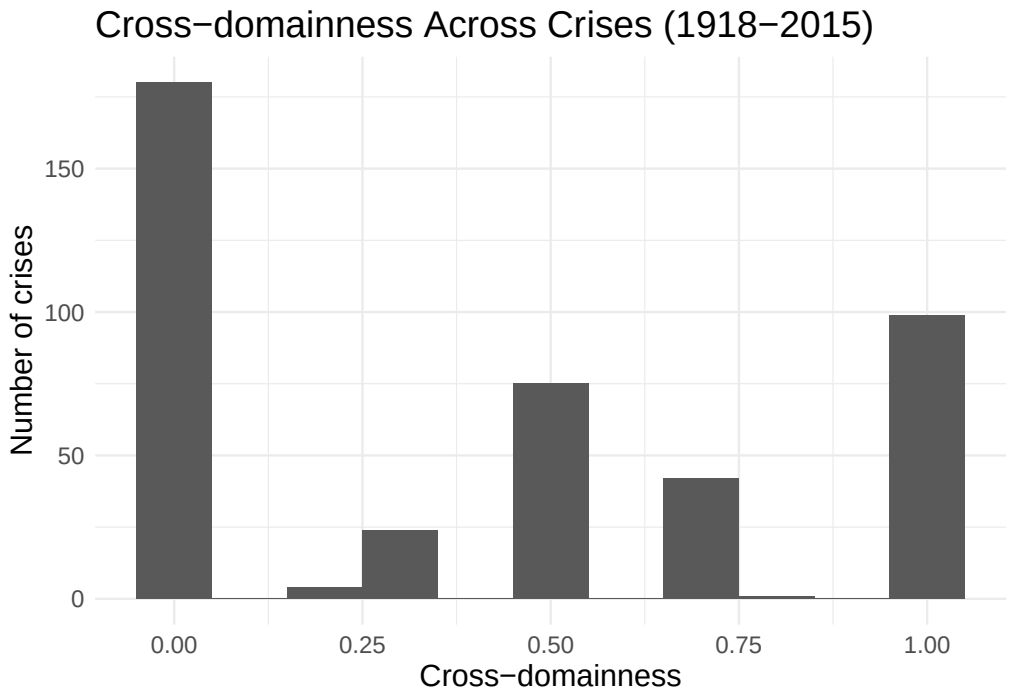

Figure 3: Distribution of cross-domainness in international crises. Higher values represent higher cross-domain interactions between adversaries

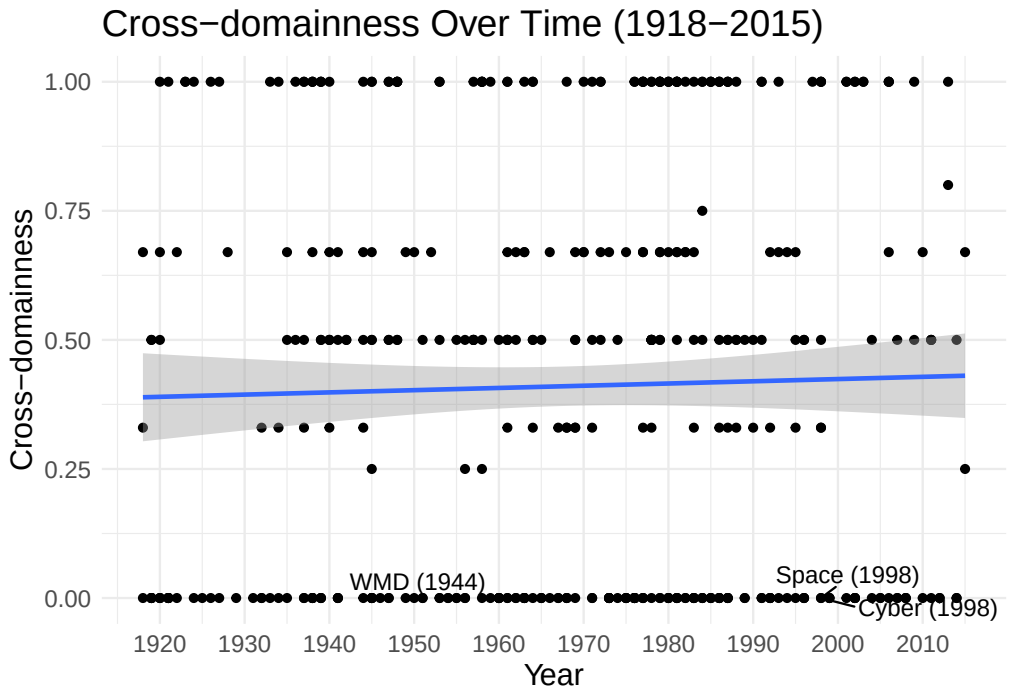

Figure 4: Distribution of cross-domainness over time. Points represent each observation (ICB crisis) and the line represents a bivariate generalized linear model with the shaded area corresponding to the 95% confidence interval. The slope is statistically insignificant. The first crises involving land, air, and sea are in the earliest year in the data (1918), while the first crises involving the other domains are labeled.

4.2 Model

To test the hypotheses about the relationship between cross-domain military interactions and crisis escalation, I model the relationship using two separate dependent variables — intensity of violence and crisis duration. These are common observable indicators for conflict escalation and intensity (Levy and Morgan 1984; Allen 2007; Asal and Beardsley 2007). The unit of analysis is the international crisis which has been collapsed down from the crisis-dyad level using the method described above.

Two different model classes are required to estimate the impact of cross-domainness on intensity of violence and crisis duration. The dependent variable for the first model — intensity of violence — is measured on an ordinal 1-4 scale with 1 describing no violence and 4 describing-full scale war. The dependent variable for the second model is crisis duration measured in days. Figure 5 shows the distribution of the dependent variables, both of which come from the original ICB crisis-level data. Because Model 1 has an ordinal dependent variable, the appropriate model specification is an ordered probit (Johnston, McDonald, and Quist 2020). Because Model 2 is a duration variable operationalized as the days from crisis initiation to crisis termination, I estimate a time accelerated hazard model with a log-normal parametric specification (Box-Steffensmeier and Jones 2004). Time accelerated hazard models have been used to estimate factors associated with the duration of interstate or intrastate conflict by Slantchev (2004), Martinez Machain (2015), and Caverley and Sechser (2017) among others.[7]

One challenge in using the crisis as the unit of analysis is conventional control variables at the actor level cannot be appropriately measured given difficulty in theoretically motivating the appropriate means of aggregation (Petersen, Vasquez, and Wang 2004, 91).[8] Nonetheless, both models include a battery of theoretically grounded control variables that influence the intensity and duration of international crises. I include a control for the number of crisis actors; more participants in an international crisis may make it more difficult to bargain peacefully, thus increasing the intensity and duration of a crisis (Petersen, Vasquez, and Wang 2004). I include a control for whether or not a crisis is part of a protracted conflict. Researchers have hypothesized that ongoing, embedded conflicts lead to more violent crises since they are part of a process that is more difficult to resolve (Azar, Jureidini, and McLaurin 1978).[9] I also include a control for whether

[7] Although other scholars have estimated a Cox proportional hazard model (Allen 2007; Beardsley and Asal 2009), the Schoenfeld residuals for my model (shown in the appendix) show that it fails the proportional hazard assumption test and is thus inappropriate (Box-Steffensmeier, Reiter, and Zorn 2003).

[8] This includes state-level variables like regime type and dyad-level variables like rivalry. There is a vast and well-developed literature on micro-foundations associated with the intensity and duration of conflict like leader traits. See, among others, McDermott (2004), Saunders (2009), Chiozza and Goemans (2011), and Horowitz and Stam (2014). I bracket discussion of the relationship between individual attributes and the choice of military domains for future research.

[9] ICB defines a protracted conflict as "an environment of ongoing disputes among adversaries, with fluctuating interaction ranging from violence to near-tranquility, multiple issues and spillover effects on all aspects of their relations, and the absence of mutually-recognized or anticipated termination (the Arab-Israeli conflict, 1947-)" (Brecher et al. 2020).

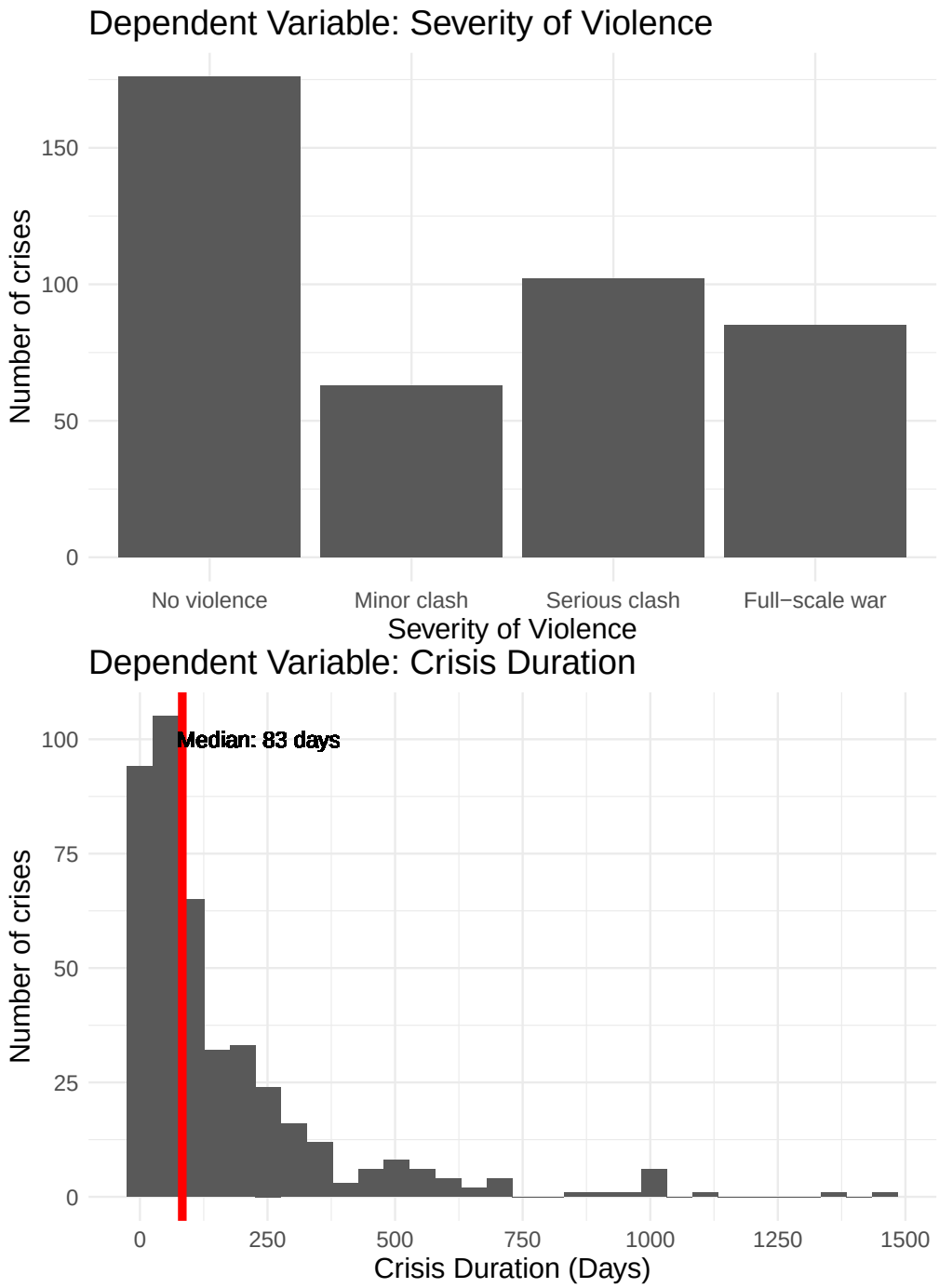

Figure 5: Distribution of dependent variables

the value that a crisis actor felt was threatened was territorial in nature since territorial conflicts like border wars are more violent and difficult to resolve (Vasquez 1995; Owsiak and Rider 2013). Territorial conflicts could also involve more similar capabilities by opposing belligerents since land and air forces may be most relevant in holding or taking territory. I include a control for whether the crisis was motivated by ethnic differences since ethnic conflicts have been shown to be more violent and difficult to resolve (Ben-Yehuda and

Mishali-Ram 2006). I include a control for the degree of power disparities between each side of a crisis, which is a composite measure of population, GNP, major power alliances, territorial size, military capability, and nuclear capability (Quinn et al. 2006). I further include a control for whether one of the two superpowers, the United States or Soviet Union, was involved in the crisis (Colaresi and Thompson 2002). Lastly, I control for contiguity which identifies whether or not the primary crisis actors share a border (Vasquez 1996).

4.3 Results

The full model results are detailed in Table 3. For each dependent variable I first estimate a bivariate model containing only "cross-domainness" as an independent variable. I then estimate full models that include all control variables. For the first two models concerning crisis intensity, the results show that cross-domainness is negatively associated with the intensity of violence with statistical significance of at least the 0.01 standardized level. As the coefficients of ordered logistic regression are difficult to interpret, the odds ratio coefficient for the cross-domainness variable (0.65) indicates that the odds of a crisis with a serious clash or full scale war are 45% lower than the odds of a crisis containing a minor clash or no violence if the actors use completely dissimilar means.[10] These results provide evidence consistent with theories of cross-domain deterrence rather than cross-domain escalation — crises in which opponents take military actions in dissimilar domains are less violent than those in which opponents take military actions in the same domains.

As models 3 and 4 are parametric time accelerated hazard models, the coefficients detail the likelihood of a crisis ending on a given day. Positive coefficients indicate a variable is associated with a longer crisis while negative coefficients mean the variable is associated with a shorter crisis duration. The coefficients for cross-domainness are negative, but not statistically significant at the 0.01 level once control variables are added to the model, meaning I cannot reject the null hypothesis that cross-domainness has no discernable effect on the duration of a crisis. The only statistically significant coefficients for crisis duration relate to the number of crisis actors and ethnic conflict. Both are statistically significant at the 0.01 level and positive, meaning that — consistent with prior research — crises with more actors and that are ethnic disputes are longer than crises with fewer actors or that involved other-than-ethnic issues.

These findings are robust across a range of alternate modeling decisions detailed in the appendix. Consistent with prior work on ICB crisis violence, I run additional models using a binary dependent variable for violence severity (Hewitt and Wilkenfeld 1996). Despite the appropriateness of ordered probit and a log-normal parametric specification for the duration model, I also find consistent results using ordered logistic and OLS regression for the severity of violence variable and using other parametric specifications for the crisis duration

[10] A complete table of the odds ratios is provided in the appendix.

	Violence Intensity		Crisis Duration	
	Model 1	Model 2	Model 3	Model 4
Cross-domainness	-0.51^{***}	-0.42^{***}	-0.30^{*}	-0.22
	(0.14)	(0.15)	(0.16)	(0.17)
No. of actors		0.08^{***}		0.07^{***}
		(0.02)		(0.02)
Power Dissimilarity		-0.00		0.00
		(0.00)		(0.01)
Protracted Crisis		0.28^{**}		-0.14
		(0.12)		(0.14)
Territorial Crisis		0.10		0.02
		(0.14)		(0.15)
Major Power Involv.		0.41^{***}		0.10
		(0.14)		(0.16)
Ethnic Crisis		0.17		0.65^{***}
		(0.13)		(0.15)
Contiguity		0.27^{*}		-0.04
		(0.15)		(0.17)
Intercept			4.45^{***}	3.82^{***}
			(0.09)	(0.22)
Log (scale)			0.29^{***}	0.24^{***}
			(0.03)	(0.04)
AIC	1111.83	922.07	5150.51	4471.94
BIC	1128.05	965.18	5162.67	4511.13
Log Likelihood	-551.91	-450.03	-2572.25	-2225.97
Deviance	1103.83	900.07		
Num. obs.	426	372	426	372

$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.
Models 1 and 2 are ordered probit models and models 3 and 4 are log-normal accelerated failure time models.

Table 3: Statistical models

dependent variable. Given the relative rarity of WMD, space, and cyber domains, I also run all models with "cross-domainness" measured excluding those three domains which produces results consistent with the original model specification.

Crises in which belligerents interact in dissimilar military domains are less violent, but neither longer nor shorter, than crises in which belligerents interact with like-means. While contemporary cross-domain conflicts with new modes of conflicts have ignited pessimism about the escalatory potential of new modes of conflict, the empirical evidence should give observers some confidence that they can respond to adversarial' "apples" with their own "oranges" without needing to be overly worried that this decision itself will result in a longer and bloodier contest. As this is a large-n observational study, it is difficult to determine the causal direction of the relationships I characterize here. This paper has proposed one mechanism by which cross-domain interactions could reduce the severity and duration of a crisis. The causal arrow may of course run the other way. It could be that the more a state cares about the outcome of a crisis, the more likely they are to bring their best military assets to the fight. Doing so may cause less blood to be spilled since bringing mobility,

stealth, and complexity to the battlefield signals to one's opponent that they are better off resolving the dispute without resorting to violence.

5 Implications of bringing a knife to a gun fight

Emerging interest in understanding cross-domain military interactions is well-deserved, given the frequency with which these interactions occur. But this research need not be spurred by, not limited to, the study of new domains made possible because of emerging technologies. Crises have always been cross-domain. Indeed, contrary to the convictions of many observers, this evidence seems to show that cross-domainness is both common and has not risen appreciably over the past century. Importantly, this suggests that theories concerning new domains of conflict need not reinvent the wheel since cross-domain interactions have themselves been a consistent regularity for the past century. At the same time, these findings point both to the need, and the ability, to better theorize cross-domain conflict. It can no longer be an excuse to claim that cross-domain conflict is too "new" to be understood even as its modality makes its understanding critical for a comprehensive appreciation of conflict processes more broadly. Different ways of defining and thinking about domains may produce new insights and certainly new domains should be compared to more traditional ones, but the findings here represent an important and thus far underrepresented contribution to that discussion.

Concerns about the escalation dynamic of cyber-kinetic interactions are loosely based off of theories of deterrence and spiral models of conflict that have rarely accounted for the strategic interaction of the military domains used by opposing sides. The common assumption held by pessimists is that cross-domain interactions risk a dangerous spiral because of potential miscommunication over proportionality, stake, and resolve. In contrast, the evidence provided here suggests that cross-domain interactions contain elements of the stability-instability paradox, where one side's willingness to operate in a new domain of conflict—a potential indicator of a willingness to escalate—creates conditions that lessen observed crisis escalation. This paper builds on the state of the art by furthering our understanding of conflict escalation. At least one part of the story in explaining why some conflicts spiral while others deter concerns the interaction between the domains in which each side's military is taking action. Although we have not witnessed many military operations in the new domains of WMD, space, and cyber in international crises, these insights help us answer the question about whether emerging technologies will make conflicts worse or whether they will prove stabilizing (Talmadge 2019). Attempts to use full-spectrum combined arms forces may make sense from a strategic standpoint if they increase the probability of victory — an outcome not examined here — but those doing so should consider preparing for a bloodier war if their opponents is not already using, or is unlikely to respond with, their own full-spectrum combined arms forces.

The escalatory effects of the tools used in a crisis are fundamental to understanding the evolution of conflict in the 21st century. These findings have implications for a number of contemporary policy debates. Recent work has investigated how other states can best combat Chinese naval expansion (Beckley 2017; Cunningham 2020). As the United States considers anti-access/anti-denial (A2/AD) in East Asia vis-a-vis competition with China, strategies that seek to take advantage of full-spectrum combined-arms forces where China does not, blending multiple military tools together as done with AirSea Battle, may invoke a less bloody contest than mirroring China's moves and operating in the same military domains that they do. As NATO considers how to respond to Russian gray zone aggression, whether "little green men" in Crimea or cyber attacks against Estonia, responding with other non-cyber or non-special operations capabilities may not be as escalatory as alarmists argued after Israel responded to Hamas cyberattacks with missile strikes. At the very least, responding to cyber attacks with actions in kinetic domains – whether raising alert levels, military mobilizations, training exercises, or shows of force – could present an ideal way to signal resolve and intent in a way that prompts a de-escalatory response rather than an escalatory one. This is not to suggest that operations in any particular domain are inherently escalatory or de-escalatory, but rather that the degree to which operations in a particular domain are escalatory or de-escalatory is at least in part a function of the domains in which one's opponent is operating.

There is much more to be studied and learned about how states fight, both as an independent variable explaining other outcomes of interest and also as a dependent variable itself. As the primary contribution of this paper concerns new data on domain-interactions over the past century, I hope part of its value comes in opening up many other avenues for research concerning questions this paper raises but does not answer. Not all cross-domain interactions are created equal. While the theories tested here concern general cross-domain escalation dynamics, a land vs air conflict may turn out differently than a land vs sea conflict, although both are quantitatively measured here as identically "cross-domain". Future work should also examine the sequence of when actors take actions in different domains, since that matters for theories of first-mover advantage and unintended escalation (Reiter 2009). Furthermore, the data as presented here makes simplifying aggregations regarding the domains in which states take actions during international crises. Future work can disaggregate both domains and actions. By looking at military units instead of domains, theories can be further refined since, for example, submarines and aircraft carriers serve different strategic purposes (Gartzke and Lindsay 2020). "Actions" can also be further disaggregated, as further work with the underlying data could parse out and evaluate differences between things like mobilizations, raises in alert level, bombardments, and occupations as well as evaluating non-actions like speeches and cognitions. The theory and findings here are also limited to military domains, but the interaction between a state's use of military, economic, and

diplomatic tools would also contribute to our collective understanding of crisis escalation and duration (Rosenau 1968; Morgan and Palmer 2000; Starr 2000). Lastly, this paper investigates military domains as an independent variable in the hopes of furthering our understanding of how the choice of military domains is associated with crisis intensity and duration. I have not explained why states choose to operate in some military domains as opposed to others. Future work should think of the military domains or crisis behavior as a dependent variable and use this novel data to explain why states choose the operate in the domains that they do.

6 Conclusion

Epidemiologists spend much of their time identifying factors that increase the risk of particular health problems in individuals. An important component of their work relies on the proper identification of events and conditions that serve as an indicator that health problems will soon follow. Similarly, scholars of international relations are interested in identifying factors that indicate that the outbreak of conflict is increasingly likely. The goal in this case is not only to causally identify factors that make war more likely so that we can better understand events of the past, but also to improve our ability to forecast the likelihood of conflict in the future. The military domains in which states contest one another and the characteristics of those domains constitutes an important piece of that puzzle. Cross-domain contests in which states engage each other with dissimilar military means are less violent and endure no longer than crises in which states respond to each other in-kind. There may be other reasons to sound the alarm over emerging technologies, but the historical record shows that responding to aggression in a new and unfamiliar domain in itself does not constitute a higher risk of conflict. Contrary to the rising sense of concern among policy practitioners and military experts, cross-domain interactions are more often associate with deterring conflict than inflaming it.

Much more needs to be done to better understand why nations invest, operate, and compete in particular domains. Often, they choose to fight in some domains and not others, despite the ability to do so. Why do some nations build big navies while others rely more heavily on land or air power? Does cyber (or space) offer significant advantages to challengers or to status quo actors? When does it make sense to pursue multi-domain conflict and when are nations better off limiting the horizontal spread of their uses of force? All of these questions require additional assessment, but begin to be within empirical reach, given the data I have presented and utilized here.

References

Allen, Susan Hannah. 2007. "Time Bombs: Estimating the Duration of Coercive Bombing Campaigns." *Journal of Conflict Resolution* 51 (1): 112–33. https://doi.org/10.1177/0022002706296153.

Allen, Susan Hannah, and Carla Martinez Machain. 2017. "Understanding the Impact of Air Power." *Conflict Management and Peace Science* 36 (5): 545–58. https://doi.org/10.1177/0738894216682485.

Althaus, Scott, Joseph Bajjalieh, John Carter, Buddy Peyton, and Dan Shalmon. 2020. "Cline Center Historical Phoenix Event Data." University of Illinois at Urbana-Champaign: Cline Center for Advanced Social Research.

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.

Asal, Victor, and Kyle Beardsley. 2007. "Proliferation and International Crisis Behavior." *Journal of Peace Research* 44 (2): 139–55. https://doi.org/10.1177/0022343307075118.

Azar, Edward E., Paul Jureidini, and Ronald McLaurin. 1978. "Protracted Social Conflict; Theory and Practice in the Middle East." *Journal of Palestine Studies* 8 (1): 41–60. https://doi.org/10.2307/2536101.

Beardsley, Kyle, and Victor Asal. 2009. "Winning with the Bomb." *Journal of Conflict Resolution* 53 (2): 278–301. https://doi.org/10.1177/0022002708330386.

Beasley, William M. 2015. "Closing the Presence GAP." *Proceedings* 141 (11): 52–58.

Beckley, Michael. 2017. "The Emerging Military Balance in East Asia: How China's Neighbors Can Check Chinese Naval Expansion." *International Security* 42 (2): 78–119. https://doi.org/10.1162/ISEC_a_00294.

Ben-Yehuda, Hemda, and Meirav Mishali-Ram. 2006. "Ethnic Actors and International Crises: Theory and Findings, 19182001." *International Interactions* 32 (1): 49–78. https://doi.org/10.1080/03050620600584435.

Biddle, Stephen, and Ivan Oelrich. 2016. "Future Warfare in the Western Pacific: Chinese Antiaccess/Area Denial, U.S. AirSea Battle, and Command of the Commons in East Asia." *International Security* 41 (1): 7–48. https://doi.org/10.1162/ISEC_a_00249.

Borghard, Erica D., and Jacquelyn Schneider. 2019. "Israel Responded to a Hamas Cyberattack with an Airstrike. That's Not Such a Big Deal." *Washington Post*, May.

Box-Steffensmeier, Janet M., and Bradford S. Jones. 2004. *Event History Modeling: A Guide for Social Scientists*. Cambridge University Press.

Box-Steffensmeier, Janet M., Dan Reiter, and Christopher Zorn. 2003. "Nonproportional Hazards and Event History Analysis in International Relations." *Journal of Conflict Resolution* 47 (1): 33–53. https://doi.org/10.1177/0022002702239510.

Brands, Hal. 2016. "Paradoxes of the Gray Zone." SSRN Scholarly Paper ID 2737593. Rochester, NY: Social Science Research Network.

Brecher, Michael, and Jonathan Wilkenfeld. 2000. *A Study of Crisis*. University of Michigan Press.

Brecher, Michael, Jonathan Wilkenfeld, Kyle C. Beardsley, Patrick James, and David Quinn. 2020. "International Crisis Behavior Data Codebook." Codebook Version 14.

Burr, William. 2005. "The Nixon Administration, the "Horror Strategy," and the Search for Limited Nuclear Options, 1969-1972: Prelude to the Schlesinger Doctrine." *Journal of Cold War Studies* 7 (3): 34–78.

Carcelli, Shannon, Rex W. Douglass, J Andrés Gannon, Erik A. Gartzke, and Thomas Leo Scherer. 2021. "Introducing the International Crisis Behavior Event (ICBe) Dataset." Working Paper.

Carcelli, Shannon, and Erik A. Gartzke. 2017. "The Diversification of Deterrence: New Data and Novel Realities." In *Oxford Research Encyclopedia of Politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.745.

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.

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.

Cashman, Greg, and Leonard C. Robinson. 2007. *An Introduction to the Causes of War: Patterns of Interstate Conflict from World War I to Iraq*. Rowman & Littlefield.

Caverley, Jonathan D, and Todd S Sechser. 2017. "Military Technology and the Duration of Civil Conflict." *International Studies Quarterly* 61 (3): 704–20. https://doi.org/10.1093/isq/sqx023.

Chiozza, Giacomo, and H. E. Goemans. 2011. *Leaders and International Conflict*. Cambridge University Press.

Cimbala, Stephen J. 1994. *Military Persuasion: Deterrence and Provocation in Crisis and War*. Pennsylvania State University Press.

Colaresi, Michael P., and William Thompson. 2002. "Strategic Rivalries, Protracted Conflict, and Crisis Escalation." *Journal of Peace Research* 39 (3): 263–87. https://doi.org/10.1177/0022343302039003002.

Cunningham, Fiona S. 2020. "The Maritime Rung on the Escalation Ladder: Naval Blockades in a US-China Conflict." *Security Studies* 29 (4): 730–68. https://doi.org/10.1080/09636412.2020.1811462.

Dafoe, Allan, Jonathan Renshon, and Paul Huth. 2014. "Reputation and Status as Motives for War." *Annual Review of Political Science* 17 (1): 371–93. https://doi.org/10.1146/annurev-polisci-071112-213421.

Duffield, John S. 1991. "The Evolution of NATO's Strategy of Flexible Response: A Reinterpretation." *Security Studies* 1 (1): 132–56. https://doi.org/10.1080/09636419109347460.

Early, Bryan R. 2014. "Exploring the Final Frontier: An Empirical Analysis of Global Civil Space Proliferation." *International Studies Quarterly* 58 (1): 55–67. https://doi.org/10.1111/isqu.12102.

Egghe, Leo. 2010. "Good Properties of Similarity Measures and Their Complementarity."

Fearon, James D. 1995. "Rationalist Explanations for War." *International Organization* 49 (3): 379–414. https://doi.org/10.1017/S0020818300033324.

Ferreiro, Larrie D. 2016. "Horatio Nelson Never Wrote 'A Ship's a Fool to Fight a Fort'; It Was Jackie Fisher Who Invented the Attribution." *Journal of Military History* 80 (3): 855–56.

Fordham, Benjamin O. 2004. "A Very Sharp Sword: The Influence of Military Capabilities on American Decisions to Use Force." *Journal of Conflict Resolution* 48 (5): 632–56. https://doi.org/10.1177/0022002704267935.

Gannon, J Andrés, Erik A. Gartzke, Jon R. Lindsay, and Peter Schram. 2021. "The Shadow of Deterrence: Why Capable Actors Engage in Contests Short of War." Working Paper.

Gartzke, Erik A. 1999. "War Is in the Error Term." *International Organization* 53 (3): 567–87. https://doi.org/10.1162/002081899550995.

Gartzke, Erik A., Shannon Carcelli, J Andrés Gannon, and Jiakun Jack Zhang. 2017. "Signaling in Foreign Policy." *Oxford Encyclopedia of Foreign Policy Analysis*, August.

Gartzke, Erik A., and Jon R. Lindsay. 2020. "The Influence of Sea Power on Politics: Domain- and Platform-Specific Attributes of Material Capabilities." *Security Studies* 29 (4): 601–36. https://doi.org/10.1080/09636412.2020.1811450.

Gavin, Francis J. 2001. "The Myth of Flexible Response: United States Strategy in Europe During the 1960s." *The International History Review* 23 (4): 847–75.

Glaser, Charles L. 1992. "Political Consequences of Military Strategy: Expanding and Refining the Spiral and Deterrence Models." *World Politics* 44 (4): 497–538. https://doi.org/10.2307/2010486.

Green, Brendan Rittenhouse. 2020. *The Revolution That Failed: Nuclear Competition, Arms Control, and the Cold War*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108779593.

Hewitt, J. Joseph. 2003. "Dyadic Processes and International Crises." *Journal of Conflict Resolution* 47 (5): 669–92. https://doi.org/10.1177/0022002703252973.

Hewitt, J. Joseph, and Jonathan Wilkenfeld. 1996. "Democracies in International Crisis." *International Interactions* 22 (2): 123–42. https://doi.org/10.1080/03050629608434885.

Hicks, Kathleen H., and Alice Hunt Friend. 2019. "By Other Means Part I: Campaigning in the Gray Zone." Lanham: Center for Strategic & International Studies.

Horowitz, Michael C. 2020. "Do Emerging Military Technologies Matter for International Politics?" *Annual Review of Political Science* 23 (1): 385–400. https://doi.org/10.1146/annurev-polisci-050718-032725.

Horowitz, Michael C., and Allan C. Stam. 2014. "How Prior Military Experience Influences the Future Militarized Behavior of Leaders." *International Organization* 68 (3): 527–59. https://doi.org/10.1017/S0020818314000046.

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

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

Johnston, Carla, James McDonald, and Kramer Quist. 2020. "A Generalized Ordered Probit Model." *Communications in Statistics - Theory and Methods* 49 (7): 1712–29. https://doi.org/10.1080/03610926.2019.1565780.

Kahn, Herman. 2007. *On Thermonuclear War*. New Brunswick [N.J.: Transaction Publishers.

Kissinger, Henry. 1960. "Limited War: Conventional or Nuclear? A Reappraisal." *Daedalus* 89 (4): 800–817.

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.

Kreps, Sarah, and Jacquelyn Schneider. 2019. "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics." *Journal of Cybersecurity* 5 (1): 1–11. https://doi.org/10.1093/cybsec/tyz007.

Kydd, Andrew. 1997. "Game Theory and the Spiral Model." *World Politics* 49 (3): 371–400.

Lai, Brian. 2004. "The Effects of Different Types of Military Mobilization on the Outcome of International Crises." *The Journal of Conflict Resolution* 48 (2): 211–29.

Levin-Banchik, Luba. 2020. "Precrisis Military Hostility and Escalation in International Crises." *Conflict Management and Peace Science* 38 (1): 63–86. https://doi.org/10.1177/0738894220906376.

Levy, Jack S., and T. Clifton Morgan. 1984. "The Frequency and Seriousness of War: An Inverse Relationship?" *Journal of Conflict Resolution* 28 (4): 731–49. https://doi.org/10.1177/0022002784028004007.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND.

———. 2012. "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society* 8: 321.

Lieber, Keir A., and Daryl G. Press. 2020. *The Myth of the Nuclear Revolution: Power Politics in the Atomic Age*. Ithaca New York: Cornell University Press.

Lindsay, Jon R., and Erik A. 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.

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

———. 2019b. "Introduction: Cross-Domain Deterrence, from Practice to Theory." In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by Jon R. Lindsay and Erik Gartzke, 1st edition, 1–26. New York, NY: Oxford University Press.

———. 2020. "Politics by Many Other Means: The Comparative Strategic Advantages of Operational Domains." *Journal of Strategic Studies* 0 (0): 1–34. https://doi.org/10.1080/01402390.2020.1768372.

Lin-Greenberg, Erik, and Theo Milonopoulos. 2021. "Private Eyes in the Sky: Emerging Technology and the Political Consequences of Eroding Government Secrecy." *Journal of Conflict Resolution*, February. https://doi.org/10.1177/0022002720987285.

Lupton, Danielle L. 2018. "Signaling Resolve: Leaders, Reputations, and the Importance of Early Interactions." *International Interactions* 44 (1): 59–87. https://doi.org/10.1080/03050629.2017.1316268.

Lyall, Jason, and Isaiah Wilson. 2009. "Rage Against the Machines: Explaining Outcomes in Counterinsurgency Wars." *International Organization* 63 (1): 67–106. https://doi.org/10.1017/S0020818309090031.

Martinez Machain, Carla. 2015. "Air Campaign Duration and the Interaction of Air and Ground Forces." *International Interactions* 41 (3): 539–64. https://doi.org/10.1080/03050629.2015.1018414.

McDermott, Rose. 2004. "Prospect Theory in Political Science: Gains and Losses from the First Decade." *Political Psychology* 25 (2): 289–312. https://doi.org/10.1111/j.1467-9221.2004.00372.x.

McMaster, H. R. 2016. "Harbingers of Future War: Implications for the Army with Lieutenant General H.R. McMaster." Washington, DC.

Montgomery, Evan Braden. 2020. "Signals of Strength: Capability Demonstrations and Perceptions of Military Power." *Journal of Strategic Studies* 43 (2): 309–30. https://doi.org/10.1080/01402390.2019.1626724.

Morgan, T. Clifton. 1994. *Untying the Knot of War: A Bargaining Theory of International Crises*. Ann Arbor: University of Michigan Press.

Morgan, T. Clifton, and Glenn Palmer. 2000. "A Model of Foreign Policy Substitutability: Selecting the Right Tools for the Job(s)." *Journal of Conflict Resolution* 44 (1): 11–32. https://doi.org/10.1177/0022002700044001002.

Morris, Loveday, Ruth Eglash, and Hazem Balousha. 2019. "Israel and Gaza Militants Agree to Cease-Fire After Weekend of Violence." *Washington Post*, May.

Morrow, James. 2019. "International Law and the Common Knowledge Requirements of Cross-Domain Deterrence." In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by Jon R. Lindsay and Erik A. Gartzke, 1st edition, 187–204. New York, NY: Oxford University Press.

Nye, Joseph. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3): 44–71. https://doi.org/10.1162/ISEC_a_00266.

O'Neill, Barry. 1991. "Conflictual Moves in Bargaining: Warnings, Threats, Escalations, and Ultimatums." In *Negotiation Analysis*, edited by H. Peyton Young, 87–108. University of Michigan Press.

Owsiak, Andrew P., and Toby J. Rider. 2013. "Clearing the Hurdle: Border Settlement and Rivalry Termination." *The Journal of Politics* 75 (3): 757–72. https://doi.org/10.1017/S0022381613000595.

Petersen, Karen K., John A. Vasquez, and Yijia Wang. 2004. "Multiparty Disputes and the Probability of War, 18161992." *Conflict Management and Peace Science* 21 (2): 85–100. https://doi.org/10.1080/07388940490463898.

Post, Abigail. 2019. "Flying to Fail: Costly Signals and Air Power in Crisis Bargaining." *Journal of Conflict Resolution* 63 (4): 869–95. https://doi.org/10.1177/0022002718777043.

Powell, Robert. 1996. "Stability and the Distribution of Power." *World Politics* 48 (2): 239–67. https://doi.org/10.1353/wp.1996.0006.

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

Quek, Kai. 2013. "Are Costly Signals More Credible? Evidence from Three Experiments." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2256528.

Quinn, David, Jonathan Wilkenfeld, Kathleen Smarick, and Victor Asal. 2006. "Power Play: Mediation in Symmetric and Asymmetric International Crises." *International Interactions* 32 (4): 441–70. https://doi.org/10.1080/03050620601011107.

Reiter, Dan. 2009. *How Wars End*. Princeton University Press.

Renshon, Jonathan. 2016. "Status Deficits and War." *International Organization* 70 (3): 513–50. https://doi.org/10.1017/S0020818316000163.

Rosen, Stephen Peter. 1991. *Winning the Next War: Innovation and the Modern Military*. Cornell University Press.

Rosenau, James N. 1968. "Comparative Foreign Policy: Fad, Fantasy, or Field?" *International Studies Quarterly* 12 (3): 296–329. https://doi.org/10.2307/3013508.

Rovner, Joshua. 2020. "Give Instability a Chance?" *War on the Rocks*. https://warontherocks.com/2020/07/give-instability-a-chance/.

Sagan, Scott Douglas, and Jeremi Suri. 2003. "The Madman Nuclear Alert: Secrecy, Signaling, and Safety in October 1969." *International Security* 27 (4): 150–83.

Saunders, Elizabeth N. 2009. "Transformative Choices: Leaders and the Origins of Intervention Strategy." *International Security* 34 (2): 119–61. https://doi.org/10.1162/isec.2009.34.2.119.

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.

Schrodt, Philip A., Deborah Gerner, Ömur Yilmaz, and Dennis Hermreck. 2005. "The CAMEO (Conflict and Mediation Event Observations) Actor Coding Framework." In *American Political Science Association Annual Meeting*. Washington, DC.

Sechser, Todd S., Neil Narang, and Caitlin Talmadge. 2019. "Emerging Technologies and Strategic Stability in

Peacetime, Crisis, and War." *Journal of Strategic Studies* 42 (6): 727–35. https://doi.org/10.1080/01402390.2019.1626725.

Slantchev, Branislav L. 2004. "How Initiators End Their Wars: The Duration of Warfare and the Terms of Peace." *American Journal of Political Science* 48 (4): 813–29. https://doi.org/10.1111/j.0092-5853.2004.00103.x.

———. 2005. "Military Coercion in Interstate Crises." *American Political Science Review* 99 (4): 533–47. https://doi.org/10.1017/S0003055405051865.

———. 2011. *Military Threats: The Costs of Coercion and the Price of Peace*. Cambridge University Press.

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.

Starr, Harvey. 2000. "Substitutability in Foreign Policy: Theoretically Central, Empirically Elusive." *Journal of Conflict Resolution* 44 (1): 128–38. https://doi.org/10.1177/0022002700044001007.

Talmadge, Caitlin. 2019. "Emerging Technology and Intra-War Escalation Risks: Evidence from the Cold War, Implications for Today." *Journal of Strategic Studies* 42 (6): 864–87. https://doi.org/10.1080/01402390.2019.1631811.

Tannenwald, Nina. 1999. *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons Since 1945*. Cambridge University Press.

Valeriano, Brandon, and Ryan C Maness. 2014. "The Dynamics of Cyber Conflict Between Rival Antagonists, 200111." *Journal of Peace Research* 51 (3): 347–60. https://doi.org/10.1177/0022343313518940.

Vasquez, John A. 1995. "Why Do Neighbors Fight? Proximity, Interaction, or Territoriality." *Journal of Peace Research* 32 (3): 277–93.

———. 1996. "Distinguishing Rivals That Go to War from Those That Do Not: A Quantitative Comparative Case Study of the Two Paths to War." *International Studies Quarterly* 40 (4): 531–58. https://doi.org/10.2307/2600890.

Wagner, R. Harrison. 2000. "Bargaining and War." *American Journal of Political Science* 44 (3): 469–84. https://doi.org/10.2307/2669259.

Warden, John K. 2018. "Limited Nuclear War: The 21st Century Challenge for the United States." 4. Lawrence Livermore National Laboratory: Center for Global Security Research.

Zagare, Frank C., and D. Marc Kilgour. 1998. "Deterrence Theory and the Spiral Model Revisited." *Journal of Theoretical Politics* 10 (1): 59–87. https://doi.org/10.1177/0951692898010001003.