Please find my memo indicating changes made to address editor and reviewer comments. I am grateful to the editorial team and reviewer for the opportunity to revise and resubmit the manuscript, as well as for the thoughtful and enlightening feedback they have provided. I am very happy with ways the paper has improved and hope that you all feel the same way.

The memo is organized by reviewer comment:

1. Each suggested change is provided first verbatim and in "quotes"
2. My response is *indented and italicized*
3. Where appropriate, I have replicated old and new figures/tables and also pasted the new verbatim text from the manuscript/appendix highlighted in gray.

I hope this eases the process of re-reviewing the paper by minimizing back and forth between the memo and the revised manuscript. Thank you all, again.

Editorial Team review

Editorial team:"Thus, we invite you to revise your manuscript and resubmit it as a Research Note for further review. Note that the word limit for Research Notes is 8,000 words."

> *The paper has been revised to be a Research Note. The word count (including title, abstract, footnotes, captions, and citations) is now: 8,546 words*

"Spotlight your main findings early in the manuscript, following the advice of Reviewer 1."

> *The main findings are now spotlighted in the fourth paragraph of the introduction, which has been shortened. The new paragraph on the findings, also reproduced below in response to Reviewer 1's comment, are below:*
>
> [Begin paper excerpt]
>
> Cross-domain military contests are neither new nor a cause for alarm. Rather than introduce a new theory, this paper contributes to the existing theoretical debate between the deterrence and spiral models of conflict with four main findings about domains that provide empirical support for existing optimistic theories of cross-domain deterrence. First, cross-domain conflict is prevalent. Some degree of cross-domain military action occurs in 58% of crises over the past century, with 23% of crises involving completely dissimilar military actions by belligerents. Second, cross-domain conflict is not novel: the rate of "cross-domainness" has remained more-or-less constant over the past century despite the accumulation of new military domains during this time period. The number of domains available does not itself seem to have triggered a greater

reliance on cross-domain operations. Third, crises in which belligerents engage in cross-domain military conflict are no more escalatory than crises where conflict remains within a given domain. Indeed, cross-domain conflicts in crises actually appear slightly less violent than conflicts within domains. Finally, cross-domain conflict in crises does not endure appreciably longer than crises in which states respond with like-means. Taken together, these findings seem to support optimistic interpretations of the effects of cross-domain conflict and to mitigate against pessimistic fears. While data on the more salient new domains like cyber remains limited at this time and these domains may be distinct when it comes to likely casualties and the types of actors that engage, insights about cross-domain interactions in more traditional military domains should help to inform theories of conflict as they are being developed and applied to more novel domains.

[End paper excerpt]

Editorial team:"Cut most of the theory (section 2) and implications (section 5) sections, focusing on the data and how it tests the two competing explanations."

Section 2 has been shortened and no longer includes a discussion of:

- *other theories of conflict escalation*
- *origin of security dilemma debate*
- *conventional-nuclear interaction*
- *new cyber and space domains*

Instead, section 2 is now focused on just defining domains and policymaker concern about cross-domain conflict. It is reproduced below in full:

[Begin paper excerpt]

A growing number of studies seek to address the effect on escalation of how conflicts are fought. Despite manifest interest, however, there is little agreement about how to conceptualize and categorize the means by which nations fight. One approach to differentiating the 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, tactics, geography, or purpose (Lindsay and Gartzke 2019). 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 more traditional domains (Libicki 2012).

Rather than engage in ontological debates about the best way to typologize conflict behavior, domains here represent 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 domains as

distinct with distinctive (and known) advantages and disadvantages (Lindsay and Gartzke 2019). As already noted, the term "domain" is used 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 an actual conflict is whether the military means one chooses determines the likelihood of escalation. Evaluations of the importance of actions in domains has recently shifted to theorizing about interactions across domains (Lindsay and Gartzke 2019). There is suspicion that cross-domain interactions are more prevalent now because there are more (and newer) domains in which states operate. Researchers and policymakers have expressed concerns that new tools of warfare may embolden revisionist forces in world affairs (Hicks and Friend 2019), 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 (Mawdsley 2016). 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 (Allen and Martinez Machain 2018).

[End paper excerpt]

Section 5 (implications) has been shortened and no longer includes a discussion of:

- *Cyber-kinetic interaction and implications for new domains*
- *Policy implications for A2AD in East Asia and Russian gray zone conflict*
- *Avenues for future research (sequence of actions, disaggregating military units, disaggregating military actions, non-military actions, domains as a dependent variable)*

Instead, section 5 is now just focused on the empirical finding about the consistency of cross-domain interactions over time as well as the test of the deterrence vs spiral explanations of cross-domain conflict. It is reproduced in full below:

[Begin paper excerpt]

Emerging interest in understanding cross-domain conflict 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. As far back as World War II, President Roosevelt advocated high altitude precision bombing precisely because it represented a cross-domain military strategy, as "Hitler built a fortress around Europe,

but he forgot to put a roof on it." (footnote: quoted in Grant (2007).) Indeed, contrary to the convictions of many observers, the evidence provided here seems to show that cross-domainness is both common and has not risen appreciably over the past century.

Competing theories of deterrence and spiral models of conflict 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 shift conflict new domain — a potential indicator of a willingness to escalate — creates conditions that lessen observed crisis escalation. Attempts to use full-spectrum combined arms forces may increase a state's probability of victory, but those doing so should consider preparing for a bloodier war if their opponents are not already using, or are unlikely to respond with, their own full-spectrum combined arms forces.

[End paper excerpt]

Editorial team: "Clarify the presentation and discussion of the data, following the detailed advice of both reviewers."

The presentation and discussion of the data has been clarified, including figures and tables redone in alignment with suggestions, the continuous nature of the independent variable re-written, and clarification of missing data on domains actor possess included. Those are described in detail after each of the corresponding reviewer suggestions.

Editorial team: "Note also that International Studies Quarterly is committed to ensuring that scholars receive appropriate intellectual acknowledgement regardless of race, gender, class, professional standing, or other categorical attributes. Please pay particular attention to this issue when revising your citations for overlooked authors and literatures. You can easily check the gender-balance of your references by using the GBAT tool found here: https://jlsumner.shinyapps.io/syllabustool/. Using this tool, your references are approximately 21.36% woman-authored. Given the persistent gender citation gap in international relations and the increasing number of female students and faculty in the discipline, we aim for approximately 30% female citations to ensure appropriate scholarly recognition."

Significant revisions were made to the citations in this manuscript. Cutting down section 2 and section 5 resulted in numerous all-male citations being removed, as their arguments are no longer part of the manuscript. Redundant "list" citations were also modified.

More important than removing all-male citations, numerous citations to woman-authored pieces were added to the manuscript. As a result of these two changes, the

GBLAT tool now indicates that the references are approximately 29.09% woman-authored.

Of the 14 new citations, 4 are mixed co-authored and the remaining 10 are woman-authored:

1. *Allen, Susan Hannah, and Carla Martinez Machain. 2018. "Choosing Air Strikes." Journal of Global Security Studies 3 (2): 150–62. https://doi.org/10.1093/jogss/ogy005.*

2. *Carson, Austin, and Keren Yarhi-Milo. 2017. "Covert Communication: The Intelligibility and Credibility of Signaling in Secret." Security Studies 26 (1): 124–56. https://doi.org/10.1080/09636412.2017.1243921.*

3. *Chung, Neo Christopher, BłaŻej Miasojedow, Michał Startek, and Anna Gambin. 2019. "Jaccard/Tanimoto Similarity Test and Estimation Methods for Biological Presence-Absence Data." BMC Bioinformatics 20 (15): 644. https://doi.org/10.1186/s12859-019-3118-5.*

4. *Grant, Rebecca. 2007. "Return of the Bomber: The Future of Long-Range Strike." AIR FORCE ASSOCIATION ARLINGTON VA.*

5. *Lupton, Danielle L. 2020. "The Reputational Costs and Ethical Implications of Coercive Limited Air Strikes: The Fallacy of the Middle-Ground Approach." Ethics & International Affairs 34 (2): 217–28. https://doi.org/10.1017/S0892679420000209.*

6. *Macdonald, Julia, and Jacquelyn Schneider. 2019. "Battlefield Responses to New Technologies: Views from the Ground on Unmanned Aircraft." Security Studies 0 (0): 1–34. https://doi.org/10.1080/09636412.2019.1551565.*

7. *Mastro, Oriana Skylar. 2011. "Signaling and Military Provocation in Chinese National Security Strategy: A Closer Look at the Impeccable Incident." Journal of Strategic Studies 34 (2): 219–44. https://doi.org/10.1080/01402390.2011.559025.*

8. *Mawdsley, Jocelyn. 2016. "Comparing Militaries: The Challenges of Datasets and Process-Tracing." In The Routledge Companion to Military Research Methods, edited by Alison J. Williams, Neil Jenkings, Rachel Woodward, and Matthew F. Rech, 115–25.*

9. *Mehta, Rupal N. 2019. "Extended Deterrence and Assurance in an Emerging Technology Environment." Journal of Strategic Studies 0 (0): 1–25. https://doi.org/10.1080/01402390.2019.1621173.*

10. *Pettyjohn, Stacie L., and Becca Wasser. 2019. "Competing in the Gray Zone: Russian Tactics and Western Responses." Santa Monica, CA: RAND Corporation.*

11. *Rasler, Karen A., and William R. Thompson. 2006. "Contested Territory, Strategic Rivalries, and Conflict Escalation." International Studies Quarterly 50 (1): 145–67. https://doi.org/10.1111/j.1468-2478.2006.00396.x.*

12. *Talmadge, Caitlin. 2017. "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States." International Security 41 (4): 50–92. https://doi.org/10.1162/ISEC_a_00274.*

13. *Tan, Michelle. 2017. "The Multi-Domain Battle." Defense News. https://www.defensenews.com/digital-show-dailies/ausa/2016/10/03/the-multi-domain-battle/.*

14. *Vasquez, John A., and Marie T. Henehan. 2001. "Territorial Disputes and the Probability of War, 1816-1992." Journal of Peace Research 38 (2): 123–38.*

Reviewer 1

Reviewer 1: "First, the paper lacks "punch." I should note that this paper is polished and clearly written, but I emerge unenthused by the framing (albeit excited about the new data). Perhaps the author could incorporate policymaker quotes or something along those lines to liven it up a bit? I leave it up to the editors to decide whether this is necessary. This point might be related to the fact that the paper does not propose a new theory but rather relies on competing conceptions of the effectiveness of cross-domain warfare. The author proposes new data to speak to the ongoing debate between pessimists and optimists on cross-domain conflict. I have no problem with this approach. Indeed, I think it suitable to the introduction of a new dataset. However, I think this approach contributes to an underwhelming argument section."

The first half of the introduction has been re-written to add more "punch". One policymaker quote has been added to the first paragraph to be illustrative of the concern about new domains of warfare:

[Begin paper excerpt]

Increased technological sophistication has given rise to new modes of conflict as states acquire a growing number of "levers" or options through which to confront one another. During the advent of each new domain of conflict, practitioners scramble to update military strategy and technology to keep up with the now irreparably transformed landscape of war. General David Perkins, Senior Commander of Training and Doctrine Command, noted that the Cold War featured "ground forces fighting ground forces, air forces fighting air forces. Cyber didn't even exist when I was a lieutenant. What's happening now is those lines are blurring between those domains…So what we're seeing is the ability to take an activity in one domain and produce an effect or dominate another domain." (footnote: quoted in Tan 2017.) There is little consensus about whether to sound the alarm about dangerously escalatory cross-domain interactions (Pettyjohn and Wasser 2019) 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 so often occurs, 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. In part, this is due to limited empirical data concerning the conduct of conflict. While scholars have developed numerous detailed datasets of participants, duration, and outcomes to understand conflict, empirically-oriented research concerning where contests take place, within which domain, has only recently received attention (Lindsay and Gartzke 2019). Researchers 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 2017; Lupton 2020).(footnote: For work that does look at cross-domain interaction, see Martinez-Machain (2015), Macdonald and Schneider (2019), and Post (2019).)

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, this study adopts 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).(Footnote: 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.) In doing so, the study develops and introduces 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 familiar and well-regarded International Crisis Behavior dataset (Brecher and Wilkenfeld 2000).

[End paper excerpt]

Another policymaker quote has been added to the first paragraph of the conclusion to illustrate the concept that cross-domain conflict is not new. That paragraph is reproduced below:

[Begin paper excerpt]

Emerging interest in understanding cross-domain conflict 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. As far back as World War II, President Roosevelt advocated high altitude precision bombing precisely because it represented a cross-domain military strategy, as “Hitler built a fortress around Europe,

but he forgot to put a roof on it." (footnote: quoted in Grant (2007).) Indeed, contrary to the convictions of many observers, the evidence provided here seems to show that cross-domainness is both common and has not risen appreciably over the past century.

[End paper excerpt]

Reviewer 1: "The author simply needs to make their contribution clearer. S/he is making an important argument (that cross-domainness in neither new nor dangerous) but dances around the debate, almost as if hoping not to offend anyone. As one possible suggestion, the author could make it more explicit before section 3.1 that s/he is going to test two sets of competing theories. It is not 100% clear that this is the case throughout the early sections."

The second half of the introduction has been re-written to eliminate two paragraphs that danced around the importance of defining military domains and to make clear that the paper is about testing two competing theories and which theory it finds support for (the optimism theory). The re-written latter half of the introduction is re-produced below. Note that it picks up right where my response to the previous comment left off, so the complete revised introduction is composed of the previous excerpt followed by this one:

[Begin paper excerpt]

Cross-domain military contests are neither new nor a cause for alarm. Rather than introduce a new theory, this paper contributes to the existing theoretical debate between the deterrence and spiral models of conflict with four main findings about domains that provide empirical support for existing optimistic theories of cross-domain deterrence. First, cross-domain conflict is prevalent. Some degree of cross-domain military action occurs in 58% of crises over the past century, with 23% of crises involving completely dissimilar military actions by belligerents. Second, cross-domain conflict is not novel: the rate of "cross-domainness" has remained more-or-less constant over the past century despite the accumulation of new military domains during this time period. The number of domains available does not itself seem to have triggered a greater reliance on cross-domain operations. Third, crises in which belligerents engage in cross-domain military conflict are no more escalatory than crises where conflict remains within a given domain. Indeed, cross-domain conflicts in crises actually appear slightly less violent than conflicts within domains. Finally, cross-domain conflict in crises does not endure appreciably longer than crises in which states respond with like-means. Taken together, these findings seem to support optimistic interpretations of the effects of cross-domain conflict and to mitigate against pessimistic fears. While data on the more salient new domains like cyber remains limited at this time and these domains may be distinct when it comes to likely casualties and the types of actors that engage, insights about cross-domain interactions in more traditional military domains should help to inform theories of conflict as they are being developed and applied to more novel domains.

This paper is organized into five sections. Section 2 outlines existing thinking concerning the domains in which states fight. Section 3 then details the existing theoretical debate between 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 concludes with the implications of these findings for theories of conflict.

[End paper excerpt]

Reviewer 1: "Figures 1 & 3 could be simplified into tables to take up less space."

Figure 1 has been replaced with tables. Below, see old Figure 1 (left) and new Table 2 (right). Figure 3 is addressed in the next comment.

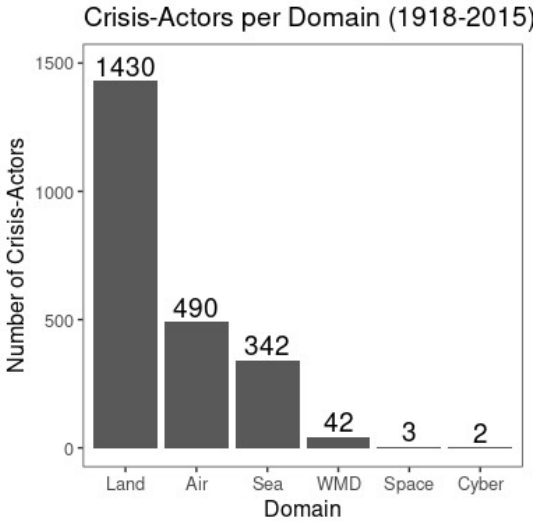
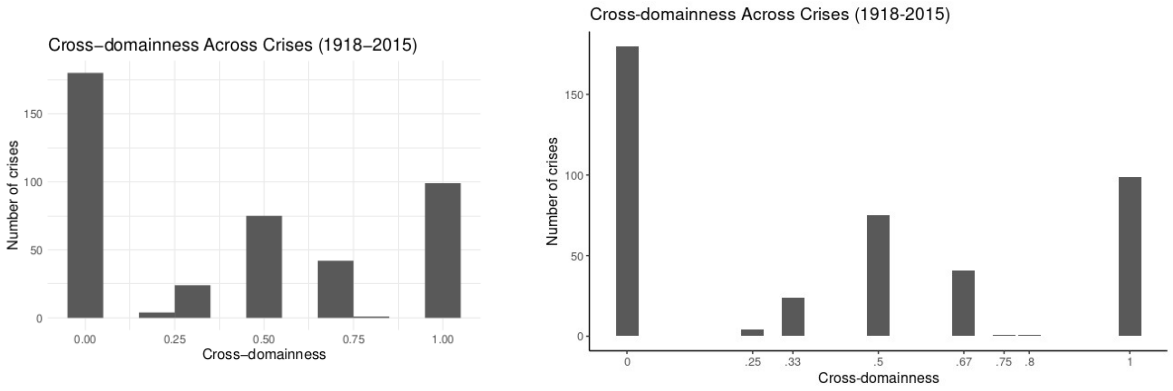


Table 2: Distribution of domains by crisis-actor

Domain	Count
Land	1,430
Air	490
Sea	342
WMD	42
Space	3
Cyber	2

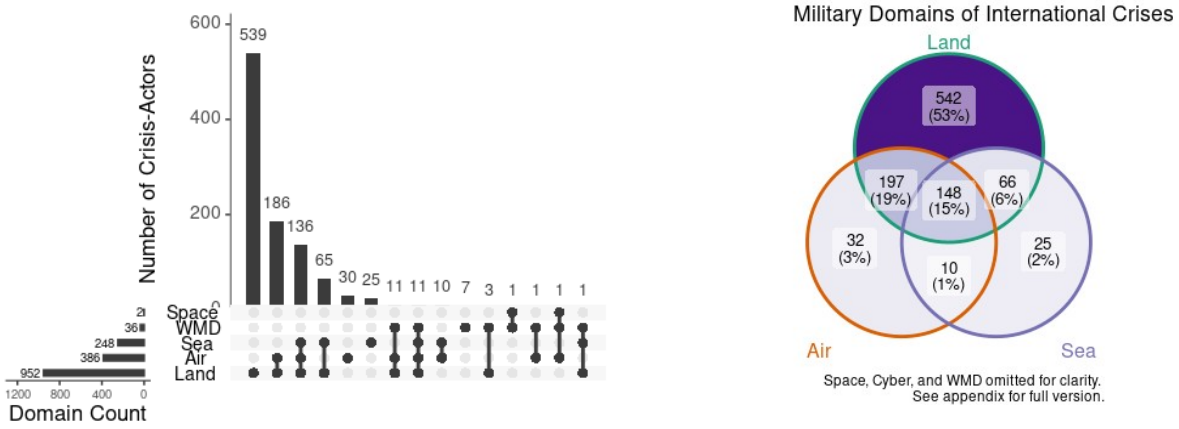
Reviewer 1: "For Figure 3, I'm unsure why there are two bars for 0.25 and 0.75. You could also label the bars."

Figure 3 has been redone by converting it from a histogram to a bar plot. The histogram was unclear since each unique value was not labeled, hence the appearance of multiple bars for 0.25 and 0.75. The new figure now labels each value, conveying that the "second bar" for 0.25 is actually the cases with a cross-domainness score of 0.33. This should better convey the continuous nature of the measure than a table would by providing a sense of the "distance" between the scores. The old figure (left) and new figure (right) are shown here:



Reviewer 1: “Figure 2 just needs to be more aesthetically pleasing with clear labels, smaller/different font, etc.”

> *Figure 2 has been redone as a simplified Venn diagram focusing on the land, air, and sea domains since they are by far the most common. The appendix includes a cleaned up version of the original plot with smaller text, clearer labels, cleaner dots, and a descriptive title. Below, see old Figure 2 (left) and new Figure 2 (right):*



Reviewer 1: “I would cut figure 5 completely or move it to the appendix. Given that the author does not code the ICB dataset, no figures of the dataset are necessary. You can easily describe them verbally in the text or just put everything into the appendix.”

> *Figure 5 has been removed from the manuscript. Instead, summary statistics for the two dependent variables are provided in Table 1 in the appendix. Below see old Figure 5 (above) and new appendix table A1 (below):*

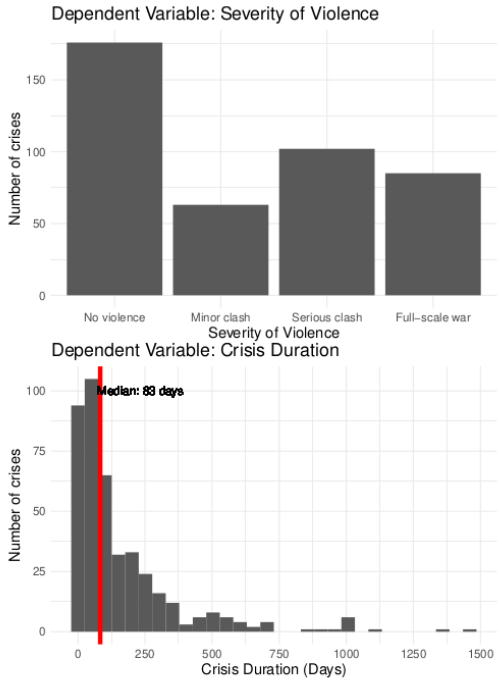


Figure 5: Distribution of dependent variables

Table A1: Covariate Summary Statistics: Crisis-actor level

Statistic	N	Mean	St. Dev.	Min	Pctl(25)	Pctl(75)	Max
Violence severity	425	2.2	1.2	1	1	3	4
Crisis duration (days)	425	163.2	214.5	1	30	203	1,461
Cross-domainness	425	0.4	0.4	0	0	0.7	1
Number of actors	425	5.6	4.0	1	3	7	34
Power discrepancy	371	8.7	13.8	0.0	2.0	11.0	179.0
Protracted conflict	425	0.6	0.5	0	0	1	1
Territorial conflict	425	0.3	0.5	0	0	1	1
Major power involv	425	0.3	0.5	0	0	1	1
Ethnic conflict	425	0.3	0.5	0	0	1	1
Contiguous	425	0.7	0.5	0	0	1	1

Reviewer 1: “When analyzing the data in Table 3, is the independent variable binary (cross-domain or no) or ordered (cross-domain at different levels)? I assume the latter based on the coding but it was unclear from the author’s discussion. Personally, I’d like to see both the binary and the ordinal measures estimated in these models. With the binary, the author could get predicted probabilities, looking at the probability of violence at each stage. This might help the author interpret the substantive effects. I use margins, margins(dydx), and marginsplot in Stata to this effect.”

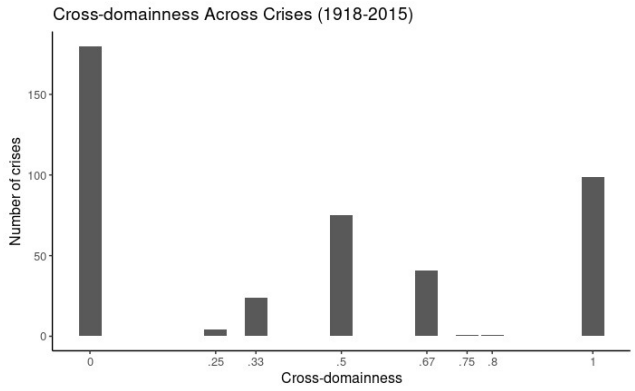
The independent variable (cross-domainness) is a continuous measure bounded between 0 and 1 where higher values represent higher cross-domainness. The first paragraph of Section 4.1.3 "Measuring cross-domainness" has been rewritten to clarify that. The revision to Figure 3 (converting the histogram to a bar plot) should also help. The new paragraph describing the measurement of the independent variable (cross-domainness) is reproduced here in full:

(Begin paper excerpt)

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. "Cross-domainness" is a continuous variable between 0 and 1, inclusive. For each crisis, if the two sides took actions in identical domains, "cross-domainess" equals 0. As the distinctiveness of the domains in which each side acted increases, the value of "cross-domainness" increases, with crises where the two sides took actions in entirely distinct domains equaling 1.

[end paper excerpt]

To the reviewer's point about a binary measure to generate predicted probabilities, the question is whether all the values of cross-domainness between 0 and 1 (non-inclusive) should be treated as 0's or as 1's:



I looked into existing research using similar measures in non-political science fields and found inconsistent suggestions. I could either consider any amount of dissimilarity as cross-domain (converting all values > 0 to 1) or consider any amount of similarity as same-domain (converting all values < 1 to 0). In other words, I would have to decide if a crisis in which one side used land + air and the other used land + sea was coded as a 0 because they both used land or coded as a 1 because air and sea were each used by only one side.

The optimism and pessimism theories don't provide a clear theoretical prior about which of those two coding decisions to take, and the results are unlikely to be the same for both coding decisions. Absent a theoretical prior, I am hesitant to run both models and then decide ex-post which makes more sense as a generalized interpretation of "cross-domain".

Reviewer 1: “Finally, I’d like to see more descriptive statistics as they relate to the actors using the various military options. Do most of the cross-domain situations involve great powers? Mostly, I’d like to know whether cross-domain military conflict is just a thing of powerful states.”

The summary statistics section of the appendix now includes 2 tables showing cross-domainness as it relates to great powers. The new text in the appendix, as well as the 2 new tables, are reproduced in full below:

[Begin appendix excerpt]

Different states could be expected to take military actions in the various domains at different frequencies. Table A2 shows that, consistent with expectations, superpowers use a wider variety of domains than small and middle powers. At the crisis-level, Table A3 shows that there is no significant difference in the amount of cross-domainness conditional on the number of great powers involved. This could occur if great power opponents in a crisis use the same domains as one another at the same rates as crises involving two non-great powers. The codings for great power status used here come from the original ICB coding and are defined in the original codebook (Brecher and Wilkenfeld 2000).

Table A2: Summary of cross-domainness by great power status

Great power status	Crisis Count	Mean Domain Count
Small power	387	1.14
Middle power	327	1.14
Great power	237	1.53
Superpower	95	1.94
NA	236	1.12

Table A3: Summary of cross-domainness in each crisis by great power involvement

Great power involvment	Crisis Count	Mean Cross-domainness
None	200	0.41
One	179	0.40
More than one	46	0.46

[End appendix excerpt]

Reviewer 2

Reviewer 2: “As it stands, the paper seems like it would make more sense as a data paper that focuses more on exploring the data. In what follows I will make several broad recommendations that I believe will help the author in revising this manuscript.”

The paper has been revised to be a research note focused on the empirical contribution and new data. Those revisions are described above in the comments to the editorial team.

Reviewer 2: "Mainly, I think that the largest problem with this manuscript is that while it discusses on page 15 that 0s (cases in which different countries did not use a particular domain) mean different things for countries that chose not to use that domain as opposed to those that were not able to use the domain, this is not further addressed in the analysis or in the theory. The author compares the similarity of domains that were used by both sides, but does not further address what it means when one side did not have a domain as an option and the other did. I bring this point up because the author is dealing with the use of domains as a signal of resolve and willingness to escalate. If the author were focusing on the effect that the use of different domains has on outcomes, I could see how it would matter less whether a state had the ability to use one type of domain versus another. Yet, when we think of the use of domains as a signal, then choosing not to expand to a new domain can also be a signal in and of itself (for example, it can be a signal of restraint that keeps the crisis from escalating). In addition, countries that are much more powerful in one domain rather than another may focus on the one domain not because they are avoiding escalation, but because they know where their comparative advantage is. Thus, I think that without considering these points, the inferences that can be drawn from the similarity of domains in which the actors engaged is somewhat limited. If this were a paper that was more focused on introducing the data itself, this problem would be avoided."

The reviewer is correct that absent data on whether an actor could have taken military action in a particular domain, the theoretical analysis is somewhat limited. I spent a few months trying to collect that data from both a newly released dataset on post-1970 military capabilities (rDMC at https://www.militarycapabilities.com/) as well as gathering original data on pre-1970 military capabilities from the Stateman's Yearbook. In doing so, I realized that still would not fully resolve the problem at the country or crisis-dyad level since regardless of what domains each side possessed, the lowest possible cross-domainness score is always 0 (land vs land can occur regardless of all the other options) and the highest possible cross-domainness score is always 1 (land vs non-land can always occur regardless of all the other options).

Incorporating the reviewer's insight would require a new measure for crises where 1) the overall combination of domains used by actor A could not have been used by actor B and 2) cases where an actor abstained from using a domain it did possess. The latter, as the reviewer notes, requires a significantly more developed theory since it requires thinking through what it means to "use" domains given research on general vs immediate deterrence (are US nuclear weapons or aircraft carriers ever really coded as a "not used"?).

To partially address this important concern, I have made the following changes to the manuscript:

1. The paper is now focused on introducing the data itself. Section 2 and the implications section have been significantly condensed and the theory section has been re-written to make clear that it is a test of existing theories of deterrence and spiral models of conflict.

2. The point about actors shifting (or consciously not shifting) to a domain where they have comparative advantage has been incorporated into the manuscript, with a caveat that empirically evaluating this claim requires data about the domains in which actors could have taken military action and that data is not available here.

[Begin paper excerpt]

While presenting your enemy with multiple dilemmas --- responding to your adversaries "rock" with "paper" --- may help you win a contest, it could also produce an incentive for your opponent to do the same --- respond again with "scissors" --- thus encouraging escalation (Talmadge 2017). It has been argued that responding in-kind --- playing rock against rock --- should be de-escalatory because it represents a symbolic gesture to opt against one's most efficient response (paper), as doing do would require the opposing side to engage in a new, even more efficient response (scissors). If an actor has a comparative advantage in a domain in which their opponent is not taking action, opting not to reap the benefits of conflict in that domain represents a refusal to escalate. (footnote: An empirical test of this argument requires data on the domains in which an actor could take military action. Although that data is not introduced in this paper, it is noted as an important area for further inquiry.) By responding in-kind, states can agree to call it a draw in a way that represents an explicit or tacit 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, p 104). Taking action in a new domain may help one side secure victory by representing a reduction in cost, but the very logic of escalation dominance that generates that outcome also means interacting in the new domain constitutes a (relative) increase in cost for one's opponent, with adverse consequences for the likelihood of a peaceful settlement (Mehta 2019). 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 implicit evidence of an opponent's unwillingness to pay the high(er) price of sticking it out, within a given domain.

[End paper excerpt]

3. I plan on continuing the data collection on domains in which states could have taken action during this time period, in the hopes that a future manuscript can develop the theory of signaling described here. Existing research (Post 2019) on signaling provides a useful starting point for thinking about domains in this respect, and applying that to the ICB data at the domain-level with distinct categorical values for (1) not owned, (2) owned + not used, and (3) owned + used.

Reviewer 2: “One area that I think is left unexplored by the author is the increased effectiveness that comes from engaging in cross-domain warfare. This point is mentioned briefly on page 21, but not really discussed at length. Given that this is something that would not really be affected by the “different zeroes” problem mentioned on page 15, I think that it would be worth exploring further. If cross-domain warfare makes victory more likely, then perhaps what is being signaled by the use of new domains is one state’s greater capabilities (which “on paper” may not be as credible of a signal).”

This is an exciting question that initially motivated the project. The difficulty is that cross-domain is a crisis-level variable that is difficult to apply to an actor-level dependent variable like victory/outcome. For cross-domainness to be an actor-level variable, the sequence of events in a crisis would have to be known. For example, if actor A first deployed land troops and then actor B responded with an aerial bombing, we could say that actor B took “cross-domain” action because their reaction was in a different domain than the initial action. But if all we know is that in a crisis, one side deployed troops and the other engaged in aerial bombing, it is not clear which actor took the crisis “out of domain”.

This issue is being addressed in a future edition of the data that does code the sequence of actions in each crisis. With the sequence coded, researchers can then code when an actor responds to an action “out of domain” as well as what action that was a response to. Unfortunately, that coding has been ongoing for over 6 years given the difficulties of coding event data at the sentence level. The author hopes that version of the broader data will be released soon, and wants this paper to be an initial demonstration of the value of domain-level data that is needed to justify continued effort into the broader project.

As an initial test, the appendix now includes a table of descriptive statistics about the number of domains an actor uses and the crisis outcome. That table and the accompanying text are reproduced below in full:

[Begin appendix excerpt]

The number of domains in which states take actions could also be an indication of their resolve, as devoting resources to more domains may indicate a greater willingness to incur costs. This could positively correlate with an actor’s probability of victory since actors who devote more resources to a conflict may be more likely to emerge victorious. Table A4 provides descriptive statistics that indicate there may be a weak positive relationship between the number of domains in which an actor takes military action and the likelihood of a positive outcome. A more sophisticated analysis would look at “relative domain count” – accounting for the number of domains their opponent used – to test theories evaluating the balance of capabilities as opposed to the balance of resolve (Powell 2015).

Table A4: Summary of Military Domains and Crisis Outcome

Actor Outcome	Count	Mean Domain Count
Defeat	224	1.21
Stalemate	229	1.33
Compromise	248	1.28
Victory	338	1.35
NA	243	1.14

[End appendix excerpt]

Reviewer 2: “Finally, I believe that by addressing the cyber domain when only two of the crisis actors in the sample use it, the paper may be extending itself too much. I understand that we can draw inferences about the cyber domain from other cross-domain uses of force, but I still think that the difference in adding air power to a ground-only campaign is different from adding land-based forces to a cyber operation. Though cyber operations are indeed aggressive and can result in people being killed, I think they are still perceived differently than more traditional uses of military force. As an example, there have recently been various cbyer attacks from foreign actors against U.S. actors. Though there has certainly been a strong public response to them, it is very different from what it would have been if these had been naval attacks against U.S. vessels, for example (even if they were attacks that did not result in any casualties).”

References to the cyber domain have been omitted from the theory section (cross-domain escalation) and from the implications section given the reviewer’s point about the uniqueness of cyber.

The introduction has also been modified to mention some of the ways in which the cyber domain is unique. It now reads as follows:

[Begin paper excerpt]

Taken together, these findings seem to support optimistic interpretations of the effects of cross-domain conflict and to mitigate against pessimistic fears. While data on the more salient new domains like cyber remains limited at this time and these domains may be distinct when it comes to likely casualties and the types of actors that engage, insights about cross-domain interactions in more traditional military domains should help to inform theories of conflict as they are being developed and applied to more novel domains.

[End paper excerpt]

Reviewer 2: “As a minor point, when the author notes (under the pessimistic theory) that cross-domain conflict makes it harder to compare proportionality, an illustrative example would be useful to clarify this point.”

An illustrative example from the Cuban Missile Crisis, originally provided by Schelling, has been provided in his discussion of the importance of "connectedness" between a response and the domain of aggression. The second half of the first paragraph of the pessimistic subsection has been re-written to this effect and is reproduced below:

[Begin paper excerpt]

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 misperceptions of capability or resolve (Morrow 2019). If a belligerent taking action with 100 ground troops is met with a defender deploying 1000 ground troops, the belligerent could reasonably 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 10 aircraft, it is less clear whether that is a raise, or instead is an effort to achieve something different, such as saving face. Schelling (1966, p. 87) describes the risk of a hypothetical example where the US responds to Soviet missiles in Cuba by quarantining Vladivostok. Because there is "a tendency to keep things in the same currency, to respond in the same language", cross-domain conflict makes it difficult for actors to ascertain their opponents resolve (Schelling 1966, p. 147). Cross-domain conflict presents actors with an "apples-to-oranges" comparison, making it more difficult potentially 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.

[End paper excerpt]

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

Anonymized author

February 08, 2022

Abstract

New domains of military conflict like space and cyber arguably increase opportunities for conflict across, as well as within, domains. Cross-domain conflict is thus seen by many as an emerging source of international instability. Yet, existing systematic empirical research has little to say about how domains interact. This study introduces a new dataset of the domains in which nations took military action during 412 international crises between 1918 and 2015. Analysis of these data yields several surprises. Far from being rare, cross-domain interactions are the modal form of conflict in crises during this period. Nor is cross-domain conflict "new:" crises that play out in more than one domain were about as frequent (proportionately) in decades past as they are today. Cross-domain crises are also less violent and of no greater duration than crises between belligerents using similar means.

Word count - 8,546

1 Introduction

Increased technological sophistication has given rise to new modes of conflict as states acquire a growing number of "levers" or options through which to confront one another. During the advent of each new domain of conflict, practitioners scramble to update military strategy and technology to keep up with the now irreparably transformed landscape of war. General David Perkins, Senior Commander of Training and Doctrine Command, noted that the Cold War featured "ground forces fighting ground forces, air forces fighting air forces. Cyber didn't even exist when I was a lieutenant. What's happening now is those lines are blurring between those domains... So what we're seeing is the ability to take an activity in one domain and produce an effect or dominate another domain."[1] There is little consensus about whether to sound the alarm about dangerously escalatory cross-domain interactions (Pettyjohn and Wasser 2019) 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 so often occurs, 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. In part, this is due to limited empirical data concerning the conduct of conflict. While scholars have developed numerous detailed datasets of participants, duration, and outcomes to understand conflict, empirically-oriented research concerning where contests take place, within which domain, has only recently received attention (Lindsay and Gartzke 2019). Researchers 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; Lupton 2020).[2]

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, this study adopts 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).[3] In doing so, the study develops and introduces a novel dataset of

[1] quoted in Tan (2017).

[2] For work that does look at cross-domain interaction, see Martinez Machain (2015), Macdonald and Schneider (2019), and Post (2019).

[3] 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

the military domains in which 1,282 crisis actors operated during 425 international crises from 1918 to 2015. These data expand on the familiar and well-regarded International Crisis Behavior dataset (Brecher and Wilkenfeld 2000).

Cross-domain military contests are neither new nor a cause for alarm. Rather than introduce a new theory, this paper contributes to the existing theoretical debate between the deterrence and spiral models of conflict with four main findings about domains that provide empirical support for existing optimistic theories of cross-domain deterrence. First, cross-domain conflict is prevalent. Some degree of cross-domain military action occurs in 58% of crises over the past century, with 23% of crises involving completely dissimilar military actions by belligerents. Second, cross-domain conflict is not novel: the rate of "cross-domainness" has remained more-or-less constant over the past century despite the accumulation of new military domains during this time period. The number of domains available does not itself seem to have triggered a greater reliance on cross-domain operations. Third, crises in which belligerents engage in cross-domain military conflict are no more escalatory than crises where conflict remains within a given domain. Indeed, cross-domain conflicts in crises actually appear slightly less violent than conflicts within domains. Finally, cross-domain conflict in crises does not endure appreciably longer than crises in which states respond with like-means. Taken together, these findings seem to support optimistic interpretations of the effects of cross-domain conflict and to mitigate against pessimistic fears. While data on the more salient new domains like cyber remains limited at this time and these domains may be distinct when it comes to likely casualties and the types of actors that engage, insights about cross-domain interactions in more traditional military domains should help to inform theories of conflict as they are being developed and applied to more novel domains.

This paper is organized into five sections. Section 2 outlines existing thinking concerning the domains in which states fight. Section 3 then details the existing theoretical debate between 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 concludes with the implications of these findings for theories of conflict.

2 Existing theories of how states fight

A growing number of studies seek to address the effect on escalation of *how* conflicts are fought. Despite manifest interest, however, there is little agreement about how to conceptualize and categorize the means

more to expose the diversity of options for conflict setting.

by which nations fight. One approach to differentiating the 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, tactics, geography, or purpose (Lindsay and Gartzke 2019). 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 more traditional domains (Libicki 2012).

Rather than engage in ontological debates about the best way to typologize conflict behavior, domains here represent 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 domains as distinct with distinctive (and known) advantages and disadvantages (Lindsay and Gartzke 2019). As already noted, the term "domain" is used 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 an actual conflict is whether the military means one chooses determines the likelihood of escalation. Evaluations of the importance of actions in domains has recently shifted to theorizing about interactions across domains (Lindsay and Gartzke 2019). There is suspicion that cross-domain interactions are more prevalent now because there are more (and newer) domains in which states operate. Researchers and policymakers have expressed concerns that new tools of warfare may embolden revisionist forces in world affairs (Hicks and Friend 2019), 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 (Mawdsley 2016). 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 (Allen and Martinez Machain 2018).

3 The Dialectic Across Domains

"A ship's a fool to fight a fort."[4] But is it wiser for a commander, or a nation, to attack a fort with another fort? Interpreting "foolish" actions as those that increase a conflict's violence and/or duration, perhaps

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

unnecessarily, this study identifies two sets of disparate expectations about cross-domain interactions. Despite contrasting predictions from 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 (Kydd 1997). 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. This section elucidates these opposing theories and develops contrasting hypotheses that the new empirical evidence on cross-domain military contests will then test.

3.1 Cross-domain escalation: the risks 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 misperceptions of capability or resolve (Morrow 2019). If a belligerent taking action with 100 ground troops is met with a defender deploying 1000 ground troops, the belligerent could reasonably 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 10 aircraft, it is less clear whether that is a raise, or instead is an effort to achieve something different, such as saving face. Schelling describes the risk of a hypothetical example where the US responds to Soviet missiles in Cuba by quarantining Vladivostok. Because there is "a tendency to keep things in the same currency, to respond in the same language," cross-domain conflict makes it difficult for actors to ascertain their opponents resolve (Schelling 1966, 147). Cross-domain conflict presents actors with an "apples-to-oranges" comparison, making it more difficult potentially 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 (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 actor has escalation dominance because of a relatively *low* value for the stakes of the conflict. Since each military domain has different strengths and weaknesses concerning outcomes like credibility, costs, signaling, and relative war fighting ability, operating in a different domain that one's adversary may signal a difference in tolerance for cost or 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 an opponent's possible domains, but disadvantages against others (Lindsay and Gartzke 2019, 16). In discussing the dangers of Chinese power projection from land, former US National Security Adviser H.R. McMaster (2016) advised practitioners to 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 a contest, it could also produce an incentive for your opponent to do the same — respond again with "scissors" — thus encouraging escalation (Talmadge 2017). It has been argued that responding in-kind — playing rock against rock — should be de-escalatory because it represents a symbolic gesture to opt against one's most efficient response (paper), as doing do would require the opposing side to engage in a new, even more efficient response (scissors). If an actor has a comparative advantage in a domain in which their opponent is not taking action, opting not to reap the benefits of conflict in that domain represents a refusal to escalate.[5] By responding in-kind, states can agree to call it a draw in a way that represents an explicit or tacit 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). Taking action in a new domain may help one side secure victory by representing a reduction in cost, but the very logic of escalation dominance that generates that outcome also means interacting in the new domain constitutes a (relative) increase in cost for one's opponent, with adverse consequences for the likelihood of a peaceful settlement (Mehta 2019). 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 implicit evidence of an opponent's unwillingness to pay the high(er) price of sticking it out, within a given domain.

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 may often share the assumption that opponents will "follow precedent by responding in kind with similar weapons against a similar target set" (Warden 2018, 24). If so, then failing to respond in kind (within domains) risks un-calibrated escalation. Scholars have raised this concern in the US-China context in arguing

[5] An empirical test of this argument requires data on the domains in which an actor *could* take military action. Although that data is not introduced in this paper, it is noted as an important area for further inquiry.

that "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).

3.2 Cross-domain deterrence: 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 or the opponent's evaluation of the stakes, a willingness to play a different game may signal that it is better to try to resolve the conflict rather than fighting. Moving to a new domain may provide a way for an actor to simultaneously signal resolve and restraint in a way that reduces the intensity and duration of a conflict that is logically similar to coordinating focal points, as witnessed with covert operations (Carson and Yarhi-Milo 2017) or firebreaks as evidenced experimentally with cyber attacks (Kreps and Schneider 2019).

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 further differ from seizing territory or discharging a rocket (Lai 2004). Operating in a new domain could deter rather than inflame by providing an avenue for graduated escalation. Reinforcing an army unit by putting bombers on alert or forward deploying a naval unit could be an incremental way of signaling resolve and a willingness to escalate without necessarily increasing the number of army troops already in context with the enemy (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 (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 (Mastro 2011). Furthermore, deterrence may work not because of mutual vulnerability, but because of one-sided fear about overwhelming punishment (Lieber and Press 2020). If operating in a new domain during a crisis indicates a state's willingness to take action in a domain where it has escalation dominance then this may convey that the state is willing to incur higher costs, so that an opponent is 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.*

In 1969, President Richard Nixon placed US nuclear bombers on alert in an attempt to signal a willingness to gradually escalate or de-escalate in response to Soviet and North Vietnamese actions (Operation Giant Lance) (Burr 2005). The example conforms with existing signaling theories in finding that some domains are better suited to turning the dial incrementally rather than all at once (Post 2019). Secretary of Defense McNamara had a similar rationale in advocating "flexible response." In the event of limited Soviet aggression, advocates hoped that a more credible threat of utilizing limited nuclear force would be sufficient to persuade the Soviet Union to back down (Duffield 1991).[6] 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). The very conditions that create a threat of immediate escalation in a cross-domain response make such an action conducive to medium and long-term de-escalation. By showing that an opponent has crossed a red line with the intensity of their aggression, a cross-domain response could convey that there are significant costs to be had if an opponent fails to pull back (Altman 2018).

Cross-domain interactions may not themselves be a direct cause of escalation (or de-escalation), but rather might represent an observable indicator for different motives to escalate in a way that masks the stakes. States with more to lose may be more willing to escalate, but cross-domain interactions may communicate this poorly, since doing so relies on an opponent identifying the costs of an adversary's action when that same action would generate different costs for themselves (Lupton 2018). Rather than try to empirically identify whether the underlying causes of cross-domain interactions directly or indirectly determine conflict intensity, the hope here is to shed light on the association between the use of these domains and crisis outcomes, whatever their origins.

4 Empirics

This section lays out the research design, empirical strategiy, and data to test they hypotheses detailed above.

[6] Experts disagree about whether Kennedy actually believed in, and would have implemented, "flexible response" or whether it was political theater (Gavin 2001). The example is meant to simply illustrate the logic used by proponents of the policy.

4.1 Research Design

The primary empirical contribution of the study is the introduction of a new dataset detailing the domains in which military actions or conflict occurred during 425 distinct crises from 1918 to 2015. The new data contain information on 1,282 crisis actors, the majority of which are states.[7] This crisis-domain dataset represents a unique source of information on the domains in which militaries operate during conflict.

The data were developed in 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, the data were re-organized at the crisis-dyad level using pre-existing work on ICB crisis-dyads as well as new codings for crisis-dyads post-2010 – the most recent year coded in pre-existing efforts. Third, a new measure was created of the dissimilarity of the domains in which each side in the crisis took military actions, a numeric measure referred to as "cross-domainness." These steps are discussed 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 basic values, 2) there is a finite timeline for responding, 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, allowing comparison of cases where a crisis did violently escalate to cases where the crisis did not. The dataset introduced contains detailed information on the military domains used by each actor during every international crisis. 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.

Project coders based their coding decisions on 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. The quality of these narratives reduces the risk 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 (a problem for the reporting of militarized interstate disputes captured by scraping news sources). The ICB narratives are also accompanied by the detailed ICB dataset, allowing the newly coded domain variables to be integrated into the broader ICB project.

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

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.

The data created here involves the domains in which states took actions during international crises.[8] 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 these data includes an aggregation of the multiple different codings that exist for each case. Table 2 shows the distribution of actions taken in each domain by each crisis actor. As expected, crisis-actors most often operate on land, 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 with which those domains have been utilized *in international crises*. This distinction is important, as existing work has documented numerous cases of cyber attacks that occur outside the universe

[8]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 (cite redacted for anonymization).

Table 2: Distribution of domains by crisis-actor

Domain	Count
Land	1,430
Air	490
Sea	342
WMD	42
Space	3
Cyber	2

of international crises defined by the International Crisis Behavior project (Gannon et al. 2021).

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 when the stakes of a conflict are increased. Figure 1 details the combination of land, air, and sea domains in which each crisis-actor took military actions.[9] While the sole deployment of land forces still remains by far the most common form of military action, combined land-air operations is the second most common, followed by land, sea, and air being used in unison.

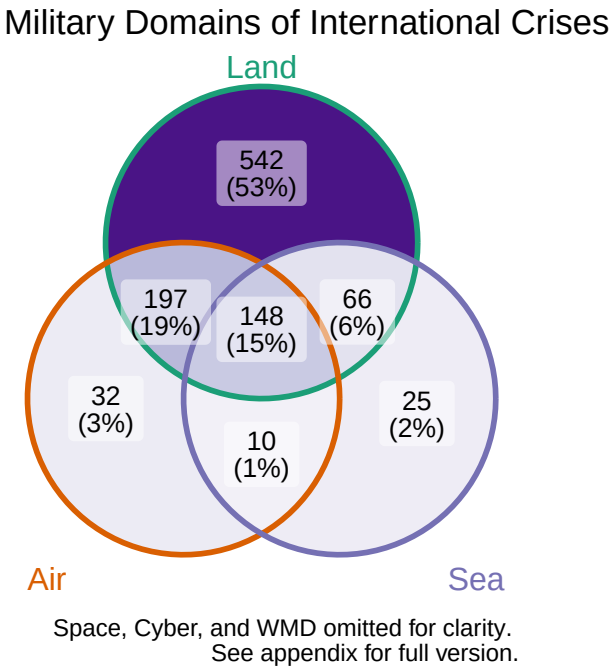


Figure 1: Intersection of domains for each crisis actor. Each bar represents the number of crisis-actors taking military action in the corresponding combination of domains

[9]The figure shows land, air, and sea as they are by far the most common and also the only domains present across the entire temporal span of the data set. See the appendix for a figure that also includes WMD, space, and cyber.

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 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. Available crisis-dyad data ends at 2010, so new codings were done for post-2010 crises. The coding followed the same rules and procedures outlined by Hewitt (2003), producing 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 domain 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. "Cross-domainness" is a continuous variable between 0 and 1, inclusive. For each crisis, if the two sides took actions in identical domains, "cross-domainess" equals 0. As the distinctiveness of the domains in which each side acted increases, the value of "cross-domainness" increases, with crises where the two sides took actions in entirely distinct domains equaling 1.

This cross-domainness measure is producing 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 3 provides descriptive examples of how domain similarity in various crises is measured. During its 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 part of military drills and kept interceptor-capable ships in the region following the drills. Since North Korea (side A) took action in the space and WMD domains, while the United States, South Korea, and Japan (side B) responded in the naval domain, the crisis was entirely cross-domain. By contrast, the 1965 Kashmir crisis involving India, Pakistan, and China consisted only of land forces. India (side A) sent troops across the ceasefire line in response to infiltration by Pakistani "freedom fighters" (side B). China (also side B) then

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 3: 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.

responded with troop movements near the border. In this case, the 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 comparison involves 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 (Chung et al. 2019). In some cases, 0's are an omission by choice (states *do not* act in this domain) but in others they represent omission by necessity (states *cannot* act in this domain). Although neither the United States nor Vietnam used WMDs during the Vietnam war, that doesn't make their military strategy similar: the United States could have done so but did not, while Vietnam could not have. Thus, 0's mean different things. This problem is avoided by measuring similarity in terms of what actors actually use, in which domain. This measurement also appropriately tests the theories presented, since they concern the consequences of states interacting in unlike ways. Similar concepts like the number of domains in which actors act are important, but are not the criteria of interest here.

Figure 2 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 sides 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 3 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.

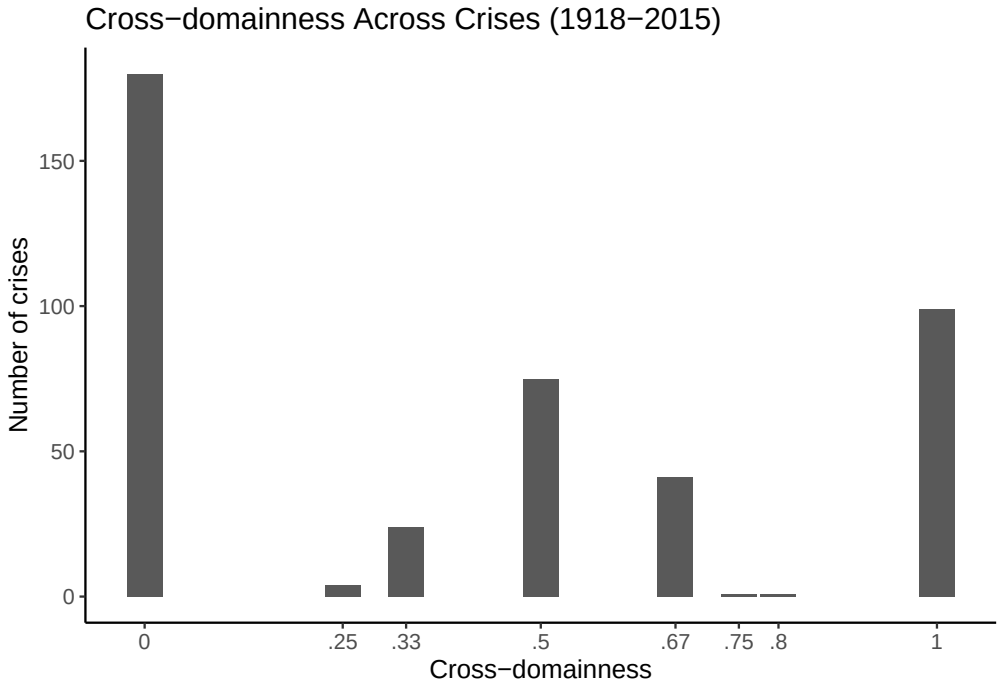


Figure 2: Distribution of cross-domainness in international crises. Higher values represent higher cross-domain interactions between adversaries

4.2 Model

To test the hypotheses about a relationship between cross-domain military interactions and crisis escalation, the relationship is modeled using two separate dependent variables — intensity of violence and crisis duration. These are common observable indicators for conflict escalation and intensity (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 (median crisis duration is 83 days‘. Because Model

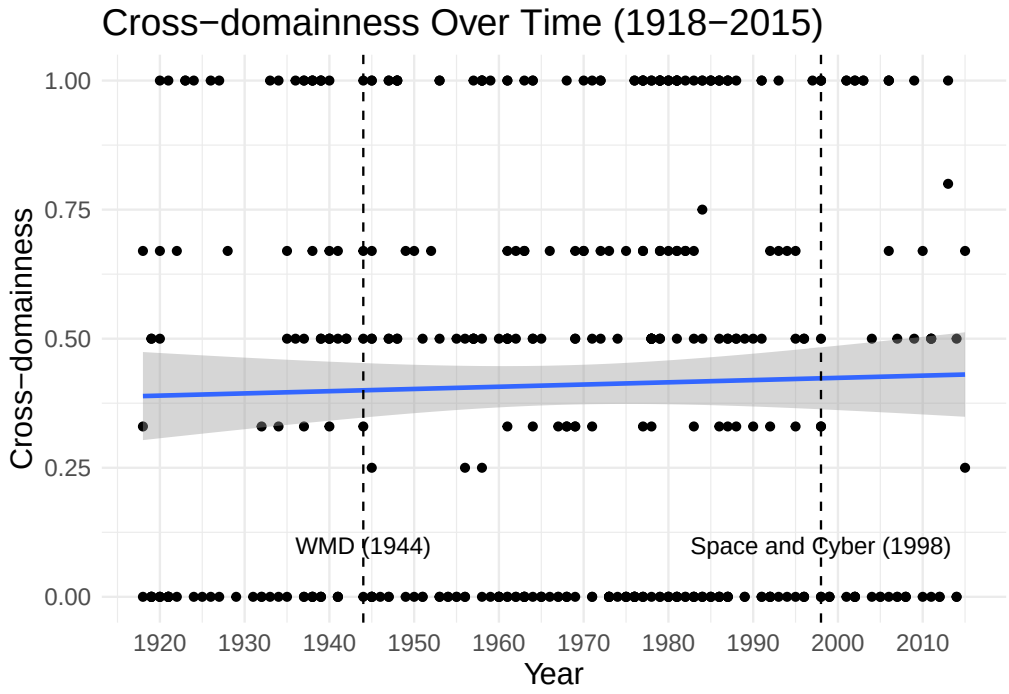


Figure 3: Distribution of cross-domainness over time. Points represent each observation (ICB crisis) and the line represents a bivariate generalized linear model with the shaded area corresponding to the 95% confidence interval. The slope is statistically insignificant. The first crises involving land, air, and sea are in the earliest year in the data (1918), while the first crises involving the other domains are labeled.

1 has an ordinal dependent variable, the appropriate model specification is an ordered probit (Johnston, McDonald, and Quist 2020). Model 2 is a duration variable operationalized as the days from crisis initiation to crisis termination, involving 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 (Martinez Machain 2015) .[10]

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).[11] Nonetheless, both models include a battery of theoretically grounded control variables that influence the intensity and duration of international crises. The models 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). There is also a control for whether or not a crisis is part of a protracted conflict. Researchers

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

[11] 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) and Saunders (2009). I bracket discussion of the relationship between individual attributes and the choice of military domains for future research.

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).[12] The models also control for whether the value that a crisis actor felt was threatened was territorial. Territorial conflicts like border wars are more violent and difficult to resolve (Vasquez and Henehan 2001). 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. The models further 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). A control is added 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). There is also 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, there is a control for contiguity which identifies whether the primary crisis actors share a border (Rasler and Thompson 2006).

4.3 Results

The full model results are detailed in Table 4. For each dependent variable, a bivariate model containing only "cross-domainness" as an independent variable is first estimated. Full models that include all control variables are then estimated. 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 at least at 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.[13] 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,. It is not possible to reject the null hypothesis that cross-domainness has no discernable

[12] 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).

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

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.

	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 4: Statistical models

These findings are robust across a range of alternate modeling decisions detailed in the appendix. Additional models are run using a binary dependent variable for violence severity. Despite the appropriateness of ordered probit and a log-normal parametric specification for the duration model, the results are also consistent using ordered logistic and OLS regression for the severity of violence variable and using other parametric specifications for the crisis duration dependent variable. Given the relative rarity of WMD, space, and cyber domains, models are also run 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 cross-domain conflicts utilizing new modes of conflict have ignited pessimism about potential instability, the empirical evidence provided here should give observers 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 characterized 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 the state is to bring its best military assets to the fight. Doing so may in turn cause less blood to be spilled since bringing mobility, stealth, and complexity to the battlefield signals to opponents that discretion may be the better part of valor, lessening violence.

5 Conclusion: Implications of bringing a knife to a gun fight

Emerging interest in understanding cross-domain conflict 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. As far back as World War II, President Roosevelt advocated high altitude precision bombing precisely because it represented a cross-domain military strategy, as "Hitler built a fortress around Europe, but he forgot to put a roof on it."[14] Indeed, contrary to the convictions of many observers, the evidence provided here seems to show that cross-domainness is both common and has not risen appreciably over the past century.

Competing theories of deterrence and spiral models of conflict 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 shift conflict new domain — a potential indicator of a willingness to escalate — creates conditions that lessen observed crisis escalation. Attempts to use full-spectrum combined arms forces may increase a state's probability of victory, but those doing so should consider preparing for a bloodier war if their opponents are not already using, or are unlikely to respond with, their own full-spectrum combined arms forces.

[14] quoted in Grant (2007).

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.

———. 2018. "Choosing Air Strikes." *Journal of Global Security Studies* 3 (2): 150–62. https://doi.org/10.1093/jogss/ogy005.

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.

Ben-Yehuda, Hemda, and Meirav Mishali-Ram. 2006. "Ethnic Actors and International Crises: Theory and Findings, 1918." *International Interactions* 32 (1): 49–78. https://doi.org/10.1080/03050620600584435.

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.

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.

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.

Carson, Austin, and Keren Yarhi-Milo. 2017. "Covert Communication: The Intelligibility and Credibility of Signaling in Secret." *Security Studies* 26 (1): 124–56. https://doi.org/10.1080/09636412.2017.1243921.

Chung, Neo Christopher, BłaŻej Miasojedow, Michał Startek, and Anna Gambin. 2019. "Jaccard/Tanimoto Similarity Test and Estimation Methods for Biological Presence-Absence Data." *BMC Bioinformatics* 20 (15): 644. https://doi.org/10.1186/s12859-019-3118-5.

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.

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.

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.

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.

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.

Grant, Rebecca. 2007. "Return of the Bomber: The Future of Long-Range Strike." AIR FORCE ASSOCIATION ARLINGTON VA.

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

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

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

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.

Libicki, Martin C. 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, eds. 2019. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. 1st edition. 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.

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.

———. 2020. "The Reputational Costs and Ethical Implications of Coercive Limited Air Strikes: The Fallacy of the Middle-Ground Approach." *Ethics & International Affairs* 34 (2): 217–28. https://doi.org/10.1017/S0892679420000209.

Macdonald, Julia, and Jacquelyn Schneider. 2019. "Battlefield Responses to New Technologies: Views from

the Ground on Unmanned Aircraft." *Security Studies* 0 (0): 1–34. https://doi.org/10.1080/09636412.2019.1551565.

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.

Mastro, Oriana Skylar. 2011. "Signaling and Military Provocation in Chinese National Security Strategy: A Closer Look at the Impeccable Incident." *Journal of Strategic Studies* 34 (2): 219–44. https://doi.org/10.1080/01402390.2011.559025.

Mawdsley, Jocelyn. 2016. "Comparing Militaries: The Challenges of Datasets and Process-Tracing." In *The Routledge Companion to Military Research Methods*, edited by Alison J. Williams, Neil Jenkings, Rachel Woodward, and Matthew F. Rech, 115–25.

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.

Mehta, Rupal N. 2019. "Extended Deterrence and Assurance in an Emerging Technology Environment." *Journal of Strategic Studies* 0 (0): 1–25. https://doi.org/10.1080/01402390.2019.1621173.

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 D. 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.

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.

Petersen, Karen K., John A. Vasquez, and Yijia Wang. 2004. "Multiparty Disputes and the Probability of War, 1816." *Conflict Management and Peace Science* 21 (2): 85–100. https://doi.org/10.1080/07388940490463898.

Pettyjohn, Stacie L., and Becca Wasser. 2019. "Competing in the Gray Zone: Russian Tactics and Western Responses." Santa Monica, CA: RAND Corporation.

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.

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.

Rasler, Karen A., and William R. Thompson. 2006. "Contested Territory, Strategic Rivalries, and Conflict Escalation." *International Studies Quarterly* 50 (1): 145–67. https://doi.org/10.1111/j.1468-2478.2006.00396.x.

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

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.

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

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

Talmadge, Caitlin. 2017. "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States." *International Security* 41 (4): 50–92. https://doi.org/10.1162/ISEC_a_00274.

———. 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.

Tan, Michelle. 2017. "The Multi-Domain Battle." *Defense News*. https://www.defensenews.com/digital-show-dailies/ausa/2016/10/03/the-multi-domain-battle/.

Vasquez, John A., and Marie T. Henehan. 2001. "Territorial Disputes and the Probability of War, 1816-1992." *Journal of Peace Research* 38 (2): 123–38.

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.