REVISE & RESUBMIT MEMORANDUM

To: Mr. Andres Gannon, Dr. Erik Gartzke & Dr. Jon Lindsay

From: Nadiya Kostyuk

Subject: "After Deterrence"

Date: December 15, 2017

I'd like thank you for sharing your paper with me. This is quite an interesting paper and I truly enjoyed reading it. In general, I think that your definition of the "gray-zone conflict" can be really influential in adding a whole new way of understanding cyber conflict and how it relates to what we know about interstate war more generally. My feedback in this memo only focuses on the areas that could be further explained and elaborated in your future work. Please use your own discretion in deciding whether to incorporate my feedback into your future drafts.

1 Theory

International norms component

By quoting a definition by Votel et al. 2016 (p.2), you bring our attention to the fact that the actions that fall into the gray zone should "undermin[e] or violat[e] international customs, norms, or laws." Later, you correctly note that "gray zone activity uses, reinforces, and changes norms." But for your illustrative cases, you use examples of cyber operations. It is worth mentioning how this usage allows states to shape cyber norms that are currently far from being adopted and agreed upon, as demonstrated by the outcome of the 2016/2017 UN GGE meeting.

Strategies as a response to the gray-zone conflict

You mention that one of the U.S. responses to the gray-zone conflict is to "counter information." What are the appropriate techniques of countering misinformation campaigns? Where is the line between countering misinformation and spreading propaganda? How applicable are these measures to other countries?

Additionally, you mention that "adapting to risk sensitivity" is another technique but you do not return to it. How was this technique achieved? Since you describe risk as an important component of your theory, it might be worth spending more time on this technique.

Actors

From the beginning, you should clearly state who the actors are. If a civil society group is executing DDoS attacks, does it mean that they are doing it on behalf of the government? Are they doing it because it is efficient? Or because they are deterred? At the beginning of your paper, you recognize that you are focusing on state actors only, but since cyberspace presents many opportunities for non-state actors to act, it might worth including a footnote that states why the non-state actors' involvement should not matter for your theory.

In your definition of the gray-zone conflict, you mention that "both actors should prefer a low-intensity conflict." Are there any situations when only one side involved in the conflict prefers a low-intensity conflict?

Your theory and definition of the gray-zone conflict is dyadic, but your illustrative cases and examples are monadic. In your theory section, you might consider explaining why you focus only on one side. Is it because it is deterred by the other side? And because of that, should the reader not care about the other – often (or always?) more powerful – side? If that is the case, your discussion of Chechen cyber operations seems to be out of place, since you bring the other side and its actions to the reader's attention.

Similarly, Table 1 provides a typology at the actor level, not the dyad level. But the definition that you mentioned earlier includes a dyad level. You might want to briefly explain why the reader should not think of the strategic interaction and should focus only on a monadic level.

Allies

Your definition of an actor (as part of an alliance) should come a bit earlier. Also, you might consider including a footnote that explains why an alliance between NATO and Ukraine, for instance, and NATO and Estonia are comparable for the purpose of your theory.

Lastly, it might be a separate topic, but reading your paper made me think of how the gray-zone conflict changes the nature of allies. Since the attribution is not always clear (or is ambiguous), are the allied countries expected to always act? If not, why does the perpetrator take the target's allies into account? You can use the above example of Ukraine and Estonia to demonstrate such differences (or resemblances).

Distinct Levels of Conflict

When discussing the distinct levels of conflict, you mention that the gray-zone conflict involves "military and political maneuvering." What is an example of such political maneuvering? By providing such examples, you can help policy makers understand when their country is in this gray-zone conflict.

Cross-domain deterrence

You mention, "One reason an actor may shift from one type of conflict to another is to shift to a domain where they opponent has a relative weakness" (p. 14). Since you have a paper that discusses cross-domain deterrence, you might want to quote it here and briefly explain its main findings in a footnote. Otherwise, this is a very interesting idea that is left unexplained here.

Definition of the gray-zone conflict

You argue that the response to actions should be in the same domain. If it is not, then the perpetrators operate in a gray-zone conflict territory. Is this always the case? If so, you should add this condition to you definition.

Deterrence versus Efficiency

Your example of the "green men" seems to demonstrate both. Most of your cases seem to include both – deterrence and efficiency. One might be more prevalent than the other.

2 Empirical Evidence

Respondent is missing

In your case selection, you do not discuss the target's response. Specifically, what the U.S. (as an ally) have done in the case of Kosovo?

Distance to DC

The distance to DC might be less relevant to this analysis (especially since you are discussing cyber operations), instead you should focus on the country's or region's importance to Russia. All cases, besides Kosovo, were in Russia's backyard. Russia might have acted differently if the countries under attack were in Western Europe, for instance. Since you already include "Russia Vital Interest" in your analysis, having both variables might be repetitive.

3 Case studies

- Georgia

  Gray-zone conflict part of traditional conflict

  You define cyber operations in the 2008 Russo-Georgian war as a gray-zone conflict. In your theory section, you should explain how a gray-zone conflict can take place along with a traditional conflict and what implications such a phenomenon has for policy-makers. This point is particularly important as we tend to think of conflicts linearly. This case study demonstrates that this is not necessarily the case.

- U.S.

  Deterrence

  Besides efficiency, deterrence played significant role in the U.S. case. Russia has chosen this strategy also because of the fear of retaliation.

- Kosovo, Chechnya and Ukraine

  Brief explanation

  You might consider briefly explaining why these case studies were included in the manuscript. You briefly explain Chechnya. Also, you mention that you do not include these cases because the cyber operations were not decisive there. But, were they decisive in the case of Georgia?

4 Stylistic Suggestions

- A new version of the joint publication was released in 2016. You might consider using that publication instead.
- "end of the conflict spectrum or maybe the military just has to adapt to new forms of limited war. Lastly is risk-confusing... (p. 4). A period was missing in the first sentence.

- "This presents 'horns of the strategic dilemma' present themselves because since the risks..." (p.4). This sentence seems to be confusing.
- However, opinions on what exactly what makes LIC distinct from conventional war differ" (p. 6). The second "what" should not be there.