Assessing Deterrence in the Gray Zone

Mr. Stephen M. Jameson
Program Manager, I2O

SBIR/STTR Industry Day
DARPA Conference Center
Arlington, VA

September 8, 2016

Objective: Assessing Deterrence in the Gray Zone

Develop and demonstrate technologies to enable measuring and explaining the success of **deterrent** strategies and tactics in **"Gray Zone"** conflicts.

Deterrence

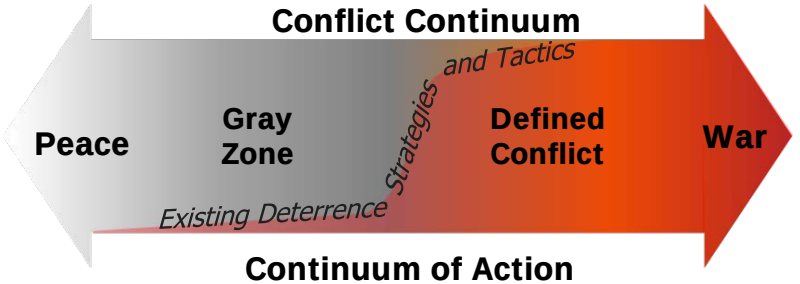
- Deterrence is a strategy intended to dissuade an adversary from undesirable action
- Deterrent options:
  - Are initiated based on evaluation of indicators of heightened regional tensions
  - Are designed to be used in groups that maximize integrated results from all the DIME instruments of national power
  - Require continuous coordination with interagency and multinational partners to maximize success

Example Deterrent Options

Diplomatic	Informational	Military	Economic
Increase cultural group pressure	Publicize violations of international law	Increase training and exercise activities	Reduce security assistance programs
Promote democratic elections	Influence adversary decision makers	Increase information operations	Encourage international corporations to restrict transactions

Gray Zone

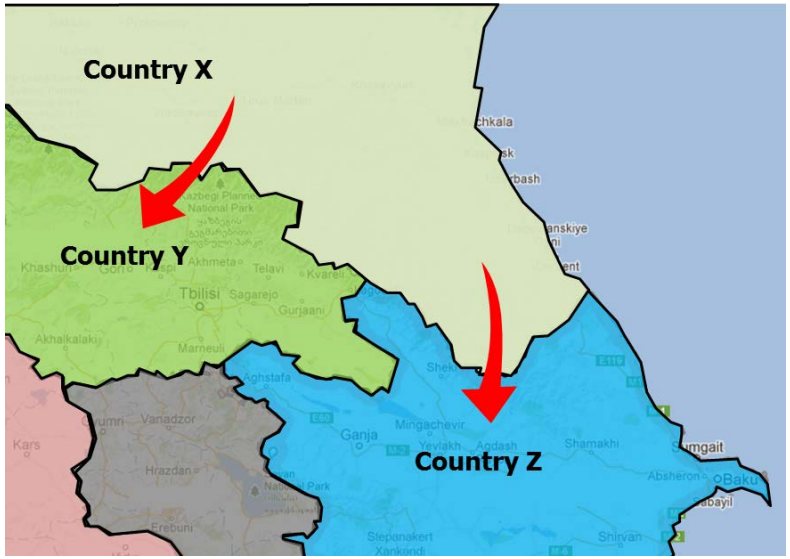
- US forces are increasingly required to operate in a segment of the conflict continuum (between war and peace) referred to as the Gray Zone
- The Gray Zone is characterized by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war



Continuum of Action
(comprised of, but not limited to)

Propaganda distribution	Diplomatic aggression
Unconventional warfare	Economic warfare
Cyber harassment	Terrorism
Covert operatives	Proxy forces

Operational Motivation



Regional aggressor Country X threatens neighbors Y and Z with a mix of unconventional actions:

- Incitement of ethnic minorities
- Economic aggression
- Cyber harassment

The US wishes to maintain regional balance and takes a set of actions to deter such “Gray Zone” activities by Country X:

- Diplomatic pressure
- Threat of economic sanctions
- Joint military exercises with Y and Z
- Public messaging

Threats from Country X abate, but:

- Did US actions cause the change in Country X behavior?
- If so, which deterrent actions were most effective?
- What other factors affected Country X behavior?
- What should we do next time?

The Problem: Assessing Deterrence in the Gray Zone

This topic seeks new technologies that can measure and explain the effectiveness of deterrent strategies in the Gray Zone leveraging open source data.

To assess the success of a deterrent, it is necessary to establish evidence that:

1. The deterrent effect was achieved ➔ Requires identifying evidence of a change in intentions on the part of the adversary
2. The deterrent action taken was a primary cause of the achieved effect ➔ Requires identifying and assessing alternative explanations for that change in intent

Both require advances over the state of the art in ability to:

- Model threat objectives and motivations
- Explain observations based on data

And require a systematic perspective that examines the complex set of conditions, actors, tactics, strategies, and outcomes across conflict holistically.

Phase 1 Overview

Phase 1 Objectives:

- Create an analytic framework that captures and incorporates the significant factors associated with deterrence in the “Gray Zone”:
  - Multiple threat or possible threat actors with identified objectives and motivations
  - Indicators of threat objectives, motivations, and actions
  - Top level characterization of operational environment (e.g. using PMESII-PT framework)
  - A broad range of possible friendly actions (e.g. defined using DIMEFIL framework)
- Build a functional subset of the analytic framework in software
- Demonstrate the ability to measure effects of selected deterrent strategies in a relevant scenario
- Define metrics and thresholds for successful assessment and demonstrate ability to measure those metrics

Think about:

- What are the novel approaches to modeling threat objectives and motivations and their observability?
- What is the appropriate level of abstraction and concomitant assumptions about upstream processing?
- What are the measures of performance and effectiveness?

Phase II Overview

Phase II Objectives:

- Design and build a prototype leveraging the Phase 1 analytic framework
- Enhance the capabilities in Phase 1 to a level of capability that can be assessed for operational utility
- Identify scenarios and data sets in conjunction with an operational partner such as a combatant command
- Conduct testing in conjunction with the partner to assess utility of the prototype capability
- Demonstrate successful performance against the metrics defined in Phase 1

Think about:

- How can indicators be identified in semantically diverse and uncertain data?
- How can the prototype best support user decision-making?
- How can thoughtful experimental design help lead to successful evaluation/assessment?

Direct to Phase II Requirements

- This SBIR topic qualifies for Direct to Phase II (DP2)
- Direct to Phase II proposals must demonstrate satisfaction of key feasibility results from Phase I definitions
  - Detailed description of Gray Zone deterrence analytic framework as described in Phase 1
  - Definition of metrics and thresholds for performance of analytic framework
  - Evidence of successful implementation and evaluation of a software prototype of the analytic framework and detailed description of results through:
    - Peer-reviewed publication
    - Deliverable report on prior funded research effort
    - Other documentation providing similar degree of detail and substantiation

Phase 3 Overview

Objectives:

- A capability that can provide a robust capability for operational users to assess and understand the effectiveness of deterrent strategies against adversaries in “Gray Zone” conflict situations
- Deployment to a combatant command in conjunction with, or integrated as part of, a suite of command and control applications in use by an operational command
- A commercializable technology for assessing and explaining adversary motivations and actions from open source data
- Dual-use applicability to strategic business decision-making applications in highly competitive industries such as information technology

Think about:

- Scalability
- Stability
- Interoperability

Deliverables: Assessing Deterrence in the Gray Zone

Phase 1

- The design for the deterrence framework
- Results of testing against the identified scenario
- A demonstration to the government
- Source code
- A report documenting research results

Phase 2

- Demonstrations to the government in each year of the Phase 2 program
- An interim report each year, and a final report at the end of Phase 2 documenting research results, the design of the demonstration prototype, and results of testing against relevant scenarios
- A plan for Phase 3 transition
- Source code for each demonstration prototype

Questions?

www.darpa.mil

stephen.jameson@darpa.mil