SAND2022-5648C

Contextualizing and Characterizing Cyber Deterrence

Using Experimental Wargaming and Theoretical Analysis to Understand the Application of Deterrence in Cyber and Hybrid Conflict Spaces

By Gabriel Kelvin (*UC Berkeley*), Dr. Bethany Goldblum (*Academic Advisor, UC Berkeley*), Dr. Kiran Lakkaraju (*Lab Mentor, Sandia National Labs*), Dr. Joshua Letchford (*Lab Mentor, Sandia National Labs*)

Nuclear Science & Security Consortium

Introduction

Deterrence in Cyber Conflict

Frameworks of deterrence in the kinetic and nuclear domains are impossible to directly apply to a cyber setting. As traditional deterrence theory is largely concerned with directly attributable state actors, geographically mappable conflict and first order effects, the absence of these conditions in the cyber domain requires new frameworks and ideals to manage cyber conflict.

The research presented here is concerned with understanding and identifying effective deterrent behaviors in the cyber domain, with additional analysis of policy interventions to allow for greater deterrence control of cyber conflict.

In order to measure behavior in a dynamic conflict setting, survey studies and qualitative analysis struggle to capture tactical and strategic behavior. Instead, experimental wargaming is used to test and evaluate hypotheses of deterrence theory.

Understanding Deterrence in Cyber Space

Modal Differences of the Cyber Domain

Cyber conflict has many fundamental differences that preclude the direct application of kinetic or nuclear deterrent theory, that are addressed in the study design. A few examples include:

Attribution Uncertainty

Identifying who perpetrated a cyber attack and what their actual intent was in relation to what actually occurred are large concerns in cyber conflict. In experimental wargaming, it is important to simulate this via delayed or partial attribution of cyber attacks, to assess both how rational actors respond to an uncertain opponent and how they use anonymity as a cover.

Effect Uncertainty

Compared to the kinetic space, cyber attacks can vary wildly with the effects of their implementation – either doing nothing at all or hitting unintended targets much harder than anticipated. In experimental wargaming, this can be modeled by cyber attacks having a great deal more variability than their traditional counterparts.

Sanctions and Threats

Reputational costs and economic sanctions are important deterrent tools in the cyber space, and in wargames, these can be simulated via threats. Players in TANTALUS may threaten their opponents to not take certain actions, and receive benefits in retaliating if their opponents take these actions anyways.

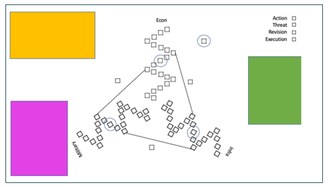
Tantalus – Experimental Wargame Development

Tantalus Wargame

Tantalus is a three-player game simulating conflict between nation-states competing across both shared and individual sectors measured by metrics. Players have the ability to either attack the metrics of their competitors through different militarist means or invest in their own, using a finite pool of resources.

Each round, players select single actions and make or receive threats from their opponents. At the end of the game, players earn "Victory Points" based on both their absolute and relative values in each metric.

Early Tantalus Game Board Prototype



Action Space

To attack their opponents, players are able to choose between kinetic, cyber or nuclear options. The differences between these domains are appear in how much damage is inflicted upon the target, how variable the effects are, and the blow-back potential they have to damage the player that launched them.

Players may also choose to invest in increasing their own metrics. For both types of actions, players can choose different levels of investment, which increases the overall effect of the action.

Threat Space

Players each round may make costly threats (spending resources) towards any of their opponents to dissuade them from taking certain actions or targeting certain metrics.

In the event that an opponent performs an action against a player that matches a threat that was made, the player receives benefits in launching a counter-attack against the aggressor.

Behaviors Across Modalities

With players having different means of attack in the conflict space, being namely kinetic, cyber and nuclear means, Tantalus allows for the identification of differences of how players perceive, use and respond to attacks from each of the three.

By analyzing differences between how players respond to their usage, deterrence behaviors and strategies, Tantalus aims to better explain and delineate the application and behavior of deterrence across multiple conflict domains.

Three-Way Conflict

The "Blue vs. Red" dichotomy present in a large amount of cyber wargaming limits analysis to two players in a largely tactical setting. By simulating a long term conflict between three players, a much more rich strategic analysis is able to be conducted by identifying how misattribution, alliances and opportunism manifest in a non-1-v-1 setting, which also allows for simulation of conflict in a more realistic, non-zero sum setting..

Attribution in Conflict

Tantalus simulates aspects of attribution uncertainty by delaying the reveal of who conducted certain actions against a player by a number of rounds.

This allows for the observation of how rational actors respond to attacks in the face of uncertainty, both militaristically and politically.

Experimental Wargaming as a Research Tool

Wargaming Study Design

Wargaming has long been used as a training tool in military settings, and simulations have often been used in cyber security settings to help train and educate employees how to respond to hostile situations in a technical setting.

However, a growing body of literature is leveraging wargaming as a study method to identify and isolating behaviors in a conflict setting.

Combining the dynamic and simulative elements of wargaming with the precision of an experimental setting, experimental wargaming differs from traditional wargaming in that it is used to identify behaviors and assess the validity of hypotheses concerning strategic behaviors in rational play.

Dynamic Behaviors

Experimental wargames differ than simple study experiments in that they allow for multiphase, strategic interaction with an intelligent opponent. This allows not only the identification of individual behaviors, but how they interact and adapt to one another in a conflict setting as they compete.

Experimental wargames offer the chance to observe how strategic interactions, player behaviors and team behaviors vary over different settings and under specified conditions.

Experimental Setting

Wargaming in the academic sense differs from traditional wargaming in that it is important to address a variety of possible confounding behaviors in players. Role playing, satisficing and skewed outlooks over large power asymmetries or "final round behaviors" require expertise to uphold an experimental setting in wargaming research.

Cyber Defense of Nuclear Infrastructure

Nuclear Cyberdefense in Practice

Further research has been conducted with the Nuclear Policy Working Group (NPWG) research team on its yearly project, "Nuclear Cyber Defense in Practice: Creating Deterrence as Far as Deterrence can be Created" which aims to create policy recommendations to better enable cyber deterrence.

The project argues that cyber conflict is currently not deterrence-enabled due to poor implementation of best practices in establishing and strengthening deterrence. Leveraging game theoretical analysis to model decision-making of actors in cyber conflict and suggesting to strengthen deterrence through consistent response and increases to cyber defense infrastructure, the project aims to make deterrence a viable strategy with the intent of protecting our Nuclear command, control & communication (NC3) infrastructure. infrastructure.

NPWG Research Team co-leads Gabriel Kelvin and Jacob Sebastian at the CSIS PONI Winter 2021 Conference, presenting "Nuclear Cyberdefense in Practice."

"Nuclear Cyberdefense in Practice" was selected to present at the Center for Strategic and International Studies' Project on Nuclear Issues Winter 2021 Conference, and will be presented as a part of its Capstone Conference, presented in partnership with U.S. Strategic Command at Offutt Airforce Base in Nebraska, May 2022.

Overview

Using game theory, the project models the behavior of cyber actors using a "simplified cyber attack expected utility model" (pictured to the right). Policy recommendations seek to maximize the potential costs and minimize the potential benefits of cyber attacks to make deterrent frameworks thus more applicable to cyberspace.

Benefits of Attack — Costs of Attack

$$u_i = p_s u_s - p_a(p_r c_r + c_a) - c_x$$

Deterrence by Denial

The first class of policy recommendations seeks to make conducting cyber attacks more difficult by instituting a policy of forward defense. By strengthening the cyber defense capabilities of nations across the world, cyber actors will face rising costs to conduct actions. Policy recommendations also cover the strategic disentanglement of nuclear infrastructure from conventional to force signaling and intentions in targeting NC3 infrastructure, raising risks of response.

Deterrence by Punishment

The second class of policy recommendations advocates for a strategy of "consistent response" of retaliation against cyber actors. With risks of retaliation remaining negligible for cyber actors, deterrence failure is inevitable, and the project seeks to balance the communication-capability tradeoff by illustrating the increased viability of cyber attacks from lack of response.

This material is based upon work supported in part by the Department of Energy National Nuclear Security Administration through the Nuclear Science and Security Consortium under Award Number DE-NA0003996.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.