DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

SAND2025-12012R

SANDIA REPORT

SAND20XX-XXXX
Printed Click to enter a date

Sandia National Laboratories

Exploring Multilayer Network Models to Build a Scientific Basis for Integrated Deterrence

Eric A. Wallace, Mathias D. Boggs, Samuel F. Gailliot, Adam D. Williams

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

The emerging multipolar international security environment represents a fundamental restructuring of global nuclear balance of power to include two nuclear peer competitors, growing non-peer nuclear threats, and concerns of nuclear latency from both allies and adversaries. Conflicts in the grey zone, cyber operations, mis- and disinformation campaigns, and emerging disruptive technologies like drones, and hypersonic missiles are becoming more prevalent. These present a risk of cross-domain and multi-domain conflicts that may not follow known escalatory patterns. In order to prepare for the new deterrence environment, it is critical to have quantitative and qualitative understandings of these cross-domain conflicts, their potential for escalation, and which systems they may impact. To that end, our team created a Multi-Layer Network (MLN) model of 'integrated deterrence' where instruments of national power are modeled as individual network graph layers that include efforts from all domains. We then evaluate the potential for escalation against escalation scenarios. Analysis of the escalation scenarios is then used to identify insights of potential risk and escalation within integrated deterrence.

ACKNOWLEDGEMENTS

We thank the comments are suggestions of Amir Mohagheghi and Jason Reinhardt during this project, their questions and insights set the tone for the research and greatly improved the final product. We also thank Annie Goodman for her efforts in the first year of this research.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

ACRONYMS AND TERMS

Acronym/Term	Definition
DOD	Department of Defense
DOE	Department of Energy
ISR	Intelligence, Surveillance, and Reconnaissance
LDRD	Laboratory Directed Research and Development
MLN	Multilayer Network Model
NNSA	National Nuclear Security Administration
NPR	Nuclear Posture Review
WMD	Weapon of Mass Destruction

1. INTRODUCTION AND RESEARCH OBJECTIVES

The emerging multipolar international security environment represents a fundamental restructuring of the nuclear order with two nuclear peer competitors, growing nuclear threats (e.g., North Korea and Iran), and concerns of nuclear latency from both allies and other adversaries. In addition, the proliferation of conventional and sub-conventional weapons (e.g. cyber operations, disinformation, artificial intelligence, machine learning, connectivity of global commerce, finance, communications, counterspace, and hypersonics) and Russian and Chinese strategies to utilize these capabilities – in combination with non-strategic nuclear weapons – to counteract U.S. conventional superiority in regional conflicts are creating novel, cross-domain, escalation pathways. Previous theories of nuclear deterrence (largely based on game theory) are ill-equipped to provide understanding of this new multiplayer, multidomain problem set.

The 2022 National Security and Defense Strategies highlight the risks of inadvertent escalation due to these changing dynamics, and advocate for the concept of integrated deterrence to mitigate these growing risks. Yet, despite greater elaboration of the concept in strategic documents, one missing element of integrated deterrence is a defendable and technical framing that provides a rigorous and structured approach for evaluating—and comparing the relative risks among—different escalatory pathways. The concept of integrated deterrence relies on the explicit and implicit interactions of domains, actors, geography, and alliances to successfully deter across a wide spectrum of adversary actions along escalatory pathways.

One of the defining characteristics of renewed strategic competition among great powers is U.S. adversary plans to counteract U.S. conventional superiority in regional conflicts. Brad Roberts argues, for example, that adversaries have "gone to school" on previous U.S. military campaigns to create their own theories of victory [1]. Three critical components of these "red" theories of victory are: (1) threatening U.S. allies in a conflict (potentially with nuclear weapons or other WMD); (2) using low-yield nuclear weapons to escalate below the U.S. nuclear threshold, forcing the United States to choose between further (possibly nuclear) escalation or capitulating without achieving its original objectives, and (3) as a last resort, striking against the U.S. homeland with conventional or nuclear weapons as a demonstration of U.S. vulnerability [2].

Concerns within the U.S. defense community about Russian and Chinese increasing conventional and nuclear capabilities, and possible strategies to create a fait accompli in regional conflicts have led to the conclusion that additional nuclear capabilities are needed to meet these new threats. The 2018 Nuclear Posture Review (NPR) notes, "To meet the emerging requirements of U.S. strategy, the United States will now pursue select enhancements to the replacement program to enhance the flexibility and responsiveness of U.S. nuclear forces… These supplements will enhance deterrence by denying potential adversaries any mistaken confidence that limited nuclear employment can provide a useful advantage over the United States and its allies [3]." The NPR further argues that the development of additional low-yield nuclear capabilities is necessary to respond at each level of the escalation ladder.

Below the threshold of armed conflict, U.S. adversaries are increasingly pursuing new ways to gain strategic advantages. These "gray zone" of "hybrid actions" actions could escalate to full conventional conflict or even a nuclear exchange, but that if left unchecked, will provide clear strategic gains to adversaries. Several scholars have noted the difficulty of addressing such threats with conventional and nuclear capabilities. The 2022 National Defense Strategy proposes the

concept of "integrated deterrence" to bring holistic capabilities to deter against such "gray zone." It defines integrated deterrence as:

> working seamlessly across warfighting domains, theaters, the spectrum of conflict, all instruments of U.S. national power, and our network of Alliances and partnerships. Tailored to specific circumstances, it applies a coordinated, multifaceted approach to reducing competitors' perceptions of the net benefits of aggression relative to restraint. Integrated deterrence is enabled by combat-credible forces prepared to fight and win, as needed, and backstopped by a safe, secure, and effective nuclear deterrent [4].

The concept of integrated deterrence demonstrates the recognition, as noted in a RAND report, that "the integration of multiple instruments of power is critical to deterrence in the gray zone [5]." Erik Gartzke and Jon Lindsay additionally note that it is "the complexity of capabilities, and the linkages among them" that are leading to "a growing number of ways to influence, with more emerging over time, and with complex interactions across options [6]." By integrating actions across multiple domains, instruments of power, phases of conflict, and alliances and partnerships [7], the United States will have a suite of tools that can be used to accomplish deterrence objectives.

Yet, despite greater elaboration of the concept in strategic documents, a crucial missing element of integrated deterrence is a defendable and technical framing that provides a rigorous and structured approach for evaluating the requirements for effective deterrence across the different domains. Traditional theories of deterrence and escalation have been built on game theory, rational actor models, and are largely dyadic. While still useful for understanding certain dynamics of nuclear deterrence, they are insufficient for a full understanding of the current political and technical environment. Unfortunately, game theoretic approaches are ill-equipped to address the complexity of additional actors and accounting for new domains are added to the problem space (nuclear, conventional, cyber, space, economic, diplomatic, etc.). In addition, while relying on the explicit and implicit interactions of domains, actors, geography, and alliances to successfully deter across a wide spectrum of adversary actions along escalatory pathways can enable new ways of influencing adversaries' perceptions of costs and benefits of taking an action, the lack of a structured approach raises concerns that escalation dynamics are not fully understood in the new strategic reality [8], [9].

Prior research examining "cross-domain deterrence" is a helpful intermediate step in understanding how threats and actions could have impacts between different domains [10]. However, this field of work is limited in several ways. First, existing literature primarily provides high-level frameworks on how to organize deterrence concepts, and the types of actions that could be taken across domains but fall short of assessing the complex relationships across domains. Second, existing cross-domain deterrence thinking points to the challenges of escalation management but fails to provide methods to understand these complex dynamics. For example, King Mallory notes that deterrence is more effective when escalation thresholds are clear, and that decision-makers should prioritize reversible, non-escalatory actions [11]. But Mallory fails to provide guidance on how to determine if certain actions are escalatory or not. Tim Sweijs and Samo Zilincik note that escalation dynamics are challenging in cross-domain deterrence because "each individual domain has a particular logic of escalation and these logics may not be inherently symbiotic [11]." Elsewhere, Sweijs et al. note that actors are able to "switch between domains but also combine the different power instruments while varying the level of intensity per domain…[to] move up and down the escalation ladder…while avoiding the threshold that would lead to open (military) conflict [12]." Ultimately, the current geopolitical and technological landscape pose challenges to traditional escalation and deterrence

theories. Rebecca Hersman notes that this new strategic environment "will require new concepts and tools to manage the risks of unintended escalation," which she poses are more like escalation "wormholes" than escalation ladders [13].

To address this gap in understanding escalation dynamics in a new strategic environment, this LDRD proposed to use multilayer network analysis methods to map the relationship between different domains and actions, examining these complex relationships between instruments of national power. Where deterrence represents a complex, multi-stakeholder problem, multilayer networks provide an analytical paradigm through which to explore a defendable, technical framing of integrated deterrence that supports coordinated, streamlined and synchronized solutions. Given that the underlying premise of integrated deterrence is the ability to use multiple levers of influence to reduce risk, network models provide a novel perspective by which to measure potential impacts on escalation dynamics. For example, an increase in military coordination among allies (e.g., increased joint armed forces exercises) could be captured as a stronger connection (a "link" in networks) between two countries ("nodes" in networks). Further, consider how nodes and links could be used to highlight the frequency and strength of geopolitical trade relationships between countries, military coordination between allies, or efforts to support nuclear nonproliferation via collaboration with international organizations.

The extent to which the link/node paradigm aligns with observed behaviors indicates how useful traditional network measures of centrality (e.g., relative importance of nodes) or minimum path length (e.g., relative efficiency of a network) can be in describing efforts to mitigate traditional and unanticipated escalation pathways. Multilayer network models expand this analytic capability with an explicit focus on the interconnections between individual layers – which can help address many of the challenges associated with clarifying cross-domain interactions in deterrence. By clearly and formally identifying linkages between layers, a multilayer network approach also provides additional opportunities to manipulate quantifiably relationships between nodes toward desired behaviors—or, at worst, manipulate the system away from undesired behaviors. More pointedly, multilayer networks can provide more holistic risk reduction—including defining, quantifying, analyzing, and optimizing multi-domain solutions for mitigating escalation pathways.

Lessons learned from other attempts to apply multilayer network models to multidomain analysis are combined with insights from complexity theory, network science, systems theory and international relations to deliver:

- A multilayer network model of integrated deterrence and cross-domain pathways
- Validation of this model through testing on historical/present case studies
- Tools needed to easily use and visualize results from these dynamic simulations

Extending the recent success Sandia has had in applying multilayer network models to high consequence facility security [38,39] integrated deterrence can be conceptualized as levers of national power from disparate domains – including, but not limited, to conventional (e.g., maritime, land, air, space) forces, nuclear forces, cyber forces, economic cooperation, trade balances, diplomatic relations, alliances, and cooperation with international organizations – modeled as individual network graphs connected by inter and intralayer links. Multilayer network models have the ability to explicitly illustrate points of interconnection between network layers and evaluate the impact of how changes in these connections impact overall performance—building on the insights and lessons learned from previous Sandia research invoking multilayer networks to help meet the Global Security investment area need for a scientific basis for integrated deterrence. Where deterrence

represents a complex problem dependent on the actions and perceptions of many stakeholders, this research project attempted to provide a defendable, technical framing that supports coordinated, streamlined and synchronized solutions.

Though limited, the success of this project provides a tool to help decision makers—at NNSA, DOD, DOE and others—assess and prioritize integrated deterrence options for improving effectiveness and reducing risks of escalation. Working towards an empirically-supported multilayer network model of integrated deterrence has better characterized traditional escalatory pathways and helped identify non-traditional escalation pathways. This increased understanding of escalation pathways will allow Sandia to further create and explore risk-informed integrated deterrence strategies, as well as evaluate risk reduction proposals prioritized on conflict pathways most likely to lead to inadvertent escalation or where adversaries have the greatest competitive advantage.

2. LITERATURE REVIEW OF INTEGRATED DETERRENCE AND ESCALATION

Since the end of the Second World War, extensive studies have focused on exploring and modeling the concepts of escalation and deterrence. To explore how multi-layer networks could be applied to the current approaches for (and challenges to) escalation and deterrence, relevant literature was reviewed according to the following four objectives:

1. Explore historical and existing approaches for enhanced understanding of escalation in cross-domain, multi-domain, and integrated deterrence scenarios.
2. Investigate applications and principles of different multi-layer network approaches for relevance.
3. Characterize options for layers, nodes, and edges to capture integrated deterrence dynamics in an associated multi-layer network.
4. Identify relevant data to support creation and analysis of an integrated deterrence multi-layer network.

2.1. Approaches for Understanding Escalation

Section 1 – "Introduction and Research Objectives" – of this report highlights the evolution of deterrence and escalation thinking, evolving from solely conventional military conflict, to nuclear conflict, and finally to competition spanning military and non-military instruments of power. As the nature of geopolitical conflict and competition has evolved, the need for models and theory that keep pace with the environmental reality has been a critical challenge.

For example, R.J. Vince [15] as noted how the "geometries" of escalation models have evolved in attempts to capture the additional complexity and nuance of escalation observed in a complex world. Vince calls out the following geometries:

- Singularity (threshold)
- Linear (ladder)
- 2D (lattice)
- 3D (space)
- Vortex
- "N" higher orders (string theory)

In the most basic geometry, thresholds are used to highlight explicitly stated red-lines (*e.g.,* use of nuclear weapons) or to explain state changes (*e.g.,* being at war or at peace). Linear models include plotting multiple events or thresholds along a single dimension, typically thought of as "vertical" escalation. The most famous of these is Herman Kahn's escalation ladder (Figure 1) [16]. This allows comparison of different activities along a single escalation axis. However, critics of the linear approach argue that it is too simplistic in explaining how escalation works, and that misperceptions and disagreements over what is more or less escalatory can lead to a failure of the model. Lo, Jie, and Lo [17] for example, suggest building escalation ladders for individual interactions, and argue that adding or removing "rungs" in the ladder (*i.e., capabilities*) can lead to strategic advantages for competitors.

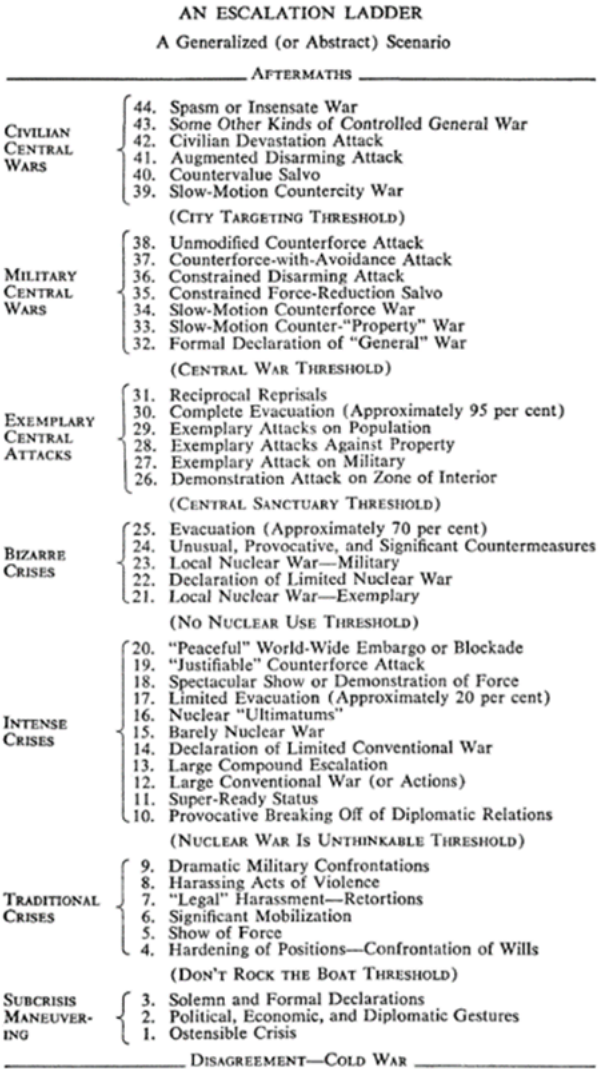


Figure 1. Herman Kahn's Escalation Ladder - An Example of a Linear Escalation Model

While linear models typically look solely at vertical escalation, treating discreet actions equally across all contexts (*e.g.,* a low-yield nuclear strike against a military base will be consistently escalatory across scenarios), additional dimensions of escalation have been explored. For example, Mallory[10] presents a 2D model that adds a "lateral escalation" axis that explores movement between different domains of warfare (Figure 2). The reason for adding this second dimension is the assertion that "each individual domain has a particular logic of escalation and these logics may not be inherently symbiotic." [18] This idea has been extensively explored, especially in regard to the unique characteristics of the cyber domain. [19, 20, 21]

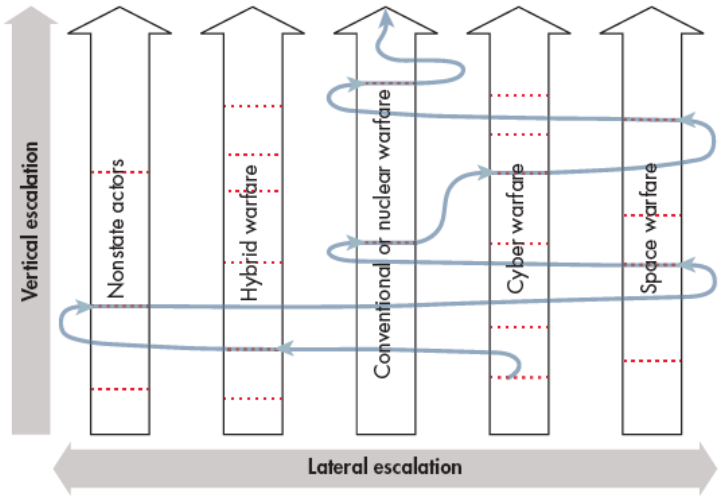


Figure 2. King Mallory's Cross-Domain Escalation Path – A 2D Escalation Model [11]

Additional complexity has been added to escalation frameworks, adding third and, as noted by Vince, "N" additional dimensions. The most common of these additional dimensions is that of geographic escalation, where expansion of conflict to different domains could be considered escalatory. Other examples include cultural perceptions and systemic and actor characteristics and context. [22, 23] The complexity of these frameworks enables them to explore and capture unique escalatory interactions in complex scenarios, but they also become more difficult to comprehend and model with each additional dimension. The simplicity of Herman Kahn's ladder, where actions are simply placed higher or lower on the vertical escalation spectrum, gives way to complex permutations of multiple different factors that try to explain what Rebecca Hersman [24] calls escalation "wormholes" created by the complex nature of conflict today.

The adaptation of the existing literature provides useful concepts and principles for understanding escalation within increasingly complex geopolitics. Yet, there is a lack of analytical tools with which to develop new theory around integrated deterrence and escalation in a multi-domain and integrated world. For this reason, this project explores the applicability of multi-layer networks in providing models of escalation in integrated conflict scenarios.

2.2. Applications and Principles of Multilayer Networks

In response, multilayer network models provide unique capabilities and functionality to help address the nuances and complexities often attributed to integrated deterrence and associated escalation dynamics. For example, the concept of integrated deterrence can be interpreted as using all instruments of national power—including but not limited to conventional military forces (e.g., maritime, land, air assets), strategic military forces (e.g., nuclear assets), cyber or communications assets, economic drivers (e.g., trade flows), and diplomatic efforts—across disparate domains to discourage certain actions by another state party. More specifically, the ability of network graphs to capture interactions between nodes and reflect relational behaviors offer a logical, well-established conceptual basis on which to model escalatory pathways that might cross traditional domains of national power projection—as well as how integrated deterrence efforts might serve in preventive or mitigatory capacities. From this perspective, leading edge evolutions in network modeling and analysis present new opportunities to address many of the challenges emerging from integrated

deterrence dialogues, including multidisciplinary interactions, non-linear dynamic relationships, and disparate time-scale synchronization.

Stated simply, network science is an academic domain with a strong tradition for describing how to identify, characterize, prioritize, analyze, and optimize interactions between elements of interest. The underlying logic of network science allows for quantitative, mathematical descriptions of these interactions as relationships (e.g., also called "links" or "edges") between these elements of interest (e.g., also called "nodes"). Not only does this framework enable evaluation of the behavior(s) of individual nodes and between pair(s) of nodes, but it also incorporates the ability to evaluate behaviors that emerge from the entire network itself [25]. The manner in which network science emphasizes both the actions of individual nodes and how they relate to one another introduce new approaches modeling escalation pathways and integrated deterrence. For example, network metrics such as minimum path length (or, the shortest geodesic distance between two given nodes in a network) and different measures of centrality (or, different perspectives on the relative importance of nodes to overall network behaviors) have the potential to better identify unexpected accelerants within different escalation models and better represent hard-to-identify cross-domain influences on escalation perceptions.

Recent efforts within network science have focused on expanding analytic capability to address increased complexity and non-linearity observed in various use cases by using multiple, connected and interacting layers within single network models [26,27,28]. These so-called *multilayer networks* (MLN) not only visualize how nodes *within* a given layer can interact, but also visualize how nodes *across* layers can interact—offering a structure to better explore unexpected, yet potentially designable, behaviors and actions. Most of the MLN development is aimed at smaller applications where there is a higher degree of homogeneity among the multiple layers to describe [29], measure [30], and evaluate [31] behaviors within—and emerging from interactions across—multiple, interacting layers. Consider two examples, social and transportation networks. From this perspective, social networks are modeled as links between social connections of a given individual, within and between separate layers each representing a separate source of the social interaction (e.g., school, work, house of worship, hobbies). Similarly, transportation networks can be modeled with locations as the nodes and the links between them representing the different modes of transportation between—capturing the dynamics resulting from the fact that travel between Boston and New York City can occur via plane, train, or automobile (including personal car, taxi, or Uber).

Such an explicit focus on structurally representing interdependence among different network layers affords a distinctive opportunity to better identify possible integrated deterrence options in response to new, novel escalation pathways—for example, how a perceived attack on a critical communications asset might initiate an unanticipated escalatory scenario. Extrapolating traditional network theoretic approaches to incorporate multiple layers introduces both expanded and new metrics by which to describe observed behaviors and actions. Consider, for example, new metrics like multilink community detection (identifying communities of nodes with many links in different layers), versatility (measuring the centrality of a node in the cohesion across all network layers), and multilayer communicability (quantifying the total number of paths joining a given node to other nodes in the MLN) [26] as new opportunities to navigate multidisciplinary interactions, non-linear dynamic relationships, and disparate time-scale synchronization among disparate network layers.

In addition, MLNs were effectively used in recent research completed by Sandia [39] to better holistically define, quantify, analyze and optimize high consequence facility security solutions.

Modeling high consequence facility security with MLNs helped leverage multiple intellectual backgrounds and normalize "security" as a socio-technical, emergent property of interacting cyber, physical, personnel, and infrastructure components. This research was a first-of-a-kind demonstration of heterogenous layers with a single MLN model and exploration of Bayesian statistics for MLN model performance. The successful results from this novel use of MLNs in a non-traditional application space demonstrated an ability to use MLN metrics to capture known (but previously not quantified) security performance measures, reinforce security performance axioms, and provide a scaffold for evolving a scientific basis for security. In summary, this research demonstrated how using MLNs can help high consequence facility security navigate dynamic and disparate time-scale synchronization between physical, cyber, personnel, and infrastructure components necessary to mitigate 21st century threats. In like manner, MLNs may be useful for tackling similar time-dependent, non-linear, and cross-domain characteristics associated with escalation pathways and integrated deterrence.

In the context of representing deterrence as a complex, multi-stakeholder problem, consider how the frequency and strength of geopolitical trade relationships between countries, military coordination between allies, and diplomatic efforts to support nuclear nonproliferation can be captured as network connections between nodes. If the underlying premise of integrated deterrence is using multiple instruments of national power to induce certain behaviors in another actor, then MLNs provide a unique structure by which to illustrate (and measure) the potential impacts of using such instruments on escalation dynamics. For example, changes in military coordination among (near) allies (e.g., increased joint armed forces exercises or joint military training) can be captured by varying the strength of links between the involved parties in a network composed of nation states. The ability to model instruments of national power as networks offers a logical structure – and associated set of metrics associated with networks – that can help identify implications or vertical and horizontal escalation.

MLN models extend this analytic usability by encouraging more specific identification of relationships between these instruments of national power as links between disparate networks to capture key concepts related to integrated deterrence and associated escalation dynamics. For example, while observation suggests that economic sanctions between countries may strain military alliances, there is currently not an explicitly defined relationship across these instruments of national power. Yet, the MLN metric "multilayer communicability" (or, a centrality measure quantifying the number of paths, within and across layers, that join a given node of a given layer to the other nodes of the multilayer structure [26]) *could* be used to deductively describe one potential relationship between economic drivers and military perception in integrated deterrence. Likewise, multilayer network page rank [26] *could* be used to reflect how a perceived stalwart of nonproliferation (a node with high centrality in a specific layer, β) that initiates a trade war (the centrality of that same node in another layer, α) could impact escalation dynamics (across all layers). Or, a metric like eigenvector versatility – which measures how much a given node supports cohesion within the multilayer model [26] – *could* be used to represent how various economic or diplomatic actions can slow escalation by identifying potential transfer points between different elements of integrated deterrence.

Taken together, the structure and analytic capabilities of MLNs can help meet the challenges of multidisciplinary, dynamism, and disparate time-scale synchronization inherent within integrated deterrence and associated escalation dynamics. MLNs provide the logical (and mathematical) structure to represent not only traditional and cross-domain relationships within, but also the multi-

time domain dynamics and emergent behaviors across instruments of national power observed (and anticipated) in executing integrated deterrence. MLN-specific metrics of node importance (e.g., eigenvector versatility or multilayer communicability), link strength (e.g., multilink community detection or multilayer path length), and overall network stability (e.g., giant connected component) all are new opportunities for better modeling integrated deterrence and associated escalation dynamics. From this perspective, MLNs can also define, quantify, and analyze (as well as potentially optimize) cross-domain solutions to more holistically model integrated deterrence and for mitigate escalation pathways to reduce risk.

2.3. Options for Multi-layer Network Structure

Perhaps the most difficult and important part of applying multi-layer networks in a new space is determining how to structure the network. Options for structuring the network were gathered through the literature review and multiple brainstorming sessions. The evolution of this discussion is captured in this section—providing a resource for future efforts also seeking to explore the use of networks and multi-layer networks for this problem space. Section 3 of this report describes in detail the approach implemented for this project.

Options for exploring MLN structures associated with escalation in integrated deterrence scenarios include:

- Layers as **Domains** – Most commonly air, land, sea, cyber, and space [32]. It is also common to make distinctions between conventional activities and weapons of mass destruction (*e.g.,* nuclear, chemical, and biological). [33] Others have suggested comparing space, cyber, conventional, and nuclear domains with hybrid warfare and nonstate actor domains. [10]
    - Domains might be used to capture the means (*e.g.,* a platform used to launch an attack) or the effects (*e.g.,* the targeted thing or where the impact is manifested). [33]
- Layers as **Instruments of Power** – Most commonly Diplomatic, Informational, Military and Economic (DIME). Additions to DIME [34] include Financial, Intelligence, Legal (DIMEFIL) [35], and Development (MIDFIELD) [34].
- Layers as **Elements of the Operating Environment** – Political, Military, Economic, Social, Information, Infrastructure (PMESII) [36].
- Layers as **Levels of conflict** – Sub-conventional, Conventional, and Strategic [24].
- Layers as **Types of deterrence** – General, Immediate, Direct, and Extended [10]
- Layers as **Vital National Interests** – Security of the Home Territory, Safety of Citizens at Home and Abroad, Economic Prosperity, and Preservation of the National Way of Life. [34]

Similarly, node and link options for exploring MLNs for escalation in integrated deterrence scenarios include:

- Actions that can be taken – *e.g.,* jamming, blinding, destroying, etc. [10]
- Functions that can be disrupted – *e.g.,* communication, reconnaissance, surveillance, etc. [10]
- Assets that can be targeted – *e.g.,* early-warning satellites, navigation satellites, communication satellites, etc.
- Countries – *e.g.,* United States, China, Russia, etc.
- Organizations – *e.g.,* Department of Defense, Department of State, United Nations, etc.

These different layer, node, and link options provide many unique permutations for exploring different aspects of deterrence and escalation.

2.4. Identify relevant data to support creation and analysis of an integrated deterrence multi-layer network

One constraint to the creation of a multi-layer network in this research area is the need for relevant and structured data. While international relations, deterrence, and escalation are complex interactions between states with broad ranges of capabilities, consistent and uniform data are critical not only for analysis of escalation scenarios, but also for the creation of the multi-layer network. Nodes, edges, and layers need to be developed consistently, and at a level that allows analysis relevant to the research question.

Based on the options identified for layers, nodes, and links in the previous section, a variety of data sources were identified as potential resources for the creation and analysis of the multi-layer network, including:

- Janes – Online and print data on military assets.
- Lowy Institute's Asia Power Index – Online website with metrics of relative power for Asia-region countries.
- Correlates of War – Online data repository capturing military and geopolitical data.
- United Nations' Comtrade – Online database capturing global trade data.

NOTE: For simplicity and clarity, this project only relied upon open, unclassified data sources.

3. MULTI-LAYER NETWORK MODELS FOR INTEGRATED DETERRENCE

The multilayer network was developed to support the analysis and evaluation of hypothetical escalation scenarios. The analysis and evaluation of these scenarios allows analysts to use both metrics related to the network structure (*e.g.,* page rank, betweenness, etc.) and external data integrated into the network, providing weights to the edges and nodes. Critically, multiplex multilayer networks – which represent one of the simplest types of multilayer networks – require nodes that are present across layers, and consistent edge types within layers. Specifically, multiplex or multi-aspect networks can be thought of as an extension of colored edge multi-graphs, where each type of edge is contained in its own network layer and inter-layer edges denote only an identity relationship.

Ultimately, to accomplish the objectives of this project, and to best use existing data that could be organized according to multi-layer network model constraints, the following design decisions were made:

- Layers – Simplified Instruments of Power (Diplomatic, Military, and Economic)
- Nodes – Countries (United States, China, Russia, Japan, Australia, Democratic People's Republic of Korea (DPRK), Republic of Korea (ROK), Taiwan, New Zealand, Pakistan, Philippines, and India.)
- Edges – Functionally defined relationships of interest between countries, contextualized against the related instrument of power (and constrained by the existence of appropriate data sources). Examples include: difference in GDP, ratio of estimated military might in region.

Data were gathered from a variety of sources. The majority of utilized data were gathered from the Lowy Institute's Asia Power Index (API) tool. These data were used for all three layers of the network. Additional trade data were gathered from the United Nations' ComTrade database, to augment the Economic layer of the network. Finally, bilateral relational data were added to the Diplomatic layer, based on methods developed during an internal Sandia project [37]. The Asia Power Index, ComTrade, and bilateral relational data were consolidated and combined into functions for each layer, as noted below.

Starting with the simplified instruments of national power, layers were created functionally. More specifically, the layers were constructed based on the data dependency within a data matrix $\boldsymbol{X}$ with $\boldsymbol{n}$ rows dedicated to individual countries and $\boldsymbol{p}$ columns containing covariates of the instruments of power. Here, a network is defined by the set $G = \{V, E\}$, where $V = \{1,\ldots,n\}$ is the set of nodes and $E = (e_{ij})_{i,j=1,\ldots,n}$ are the (weighted and hence not necessarily symmetric) edges connecting nodes *i* and *j*. Each "layer" function, $f_l(x_i)$, was evaluated for each country, where edges are obtained by comparing functions across countries using $e_{ij}^{(l)} = h_l\big(f(x_i), f(x_j)\big)$. Multilayer network layers are then generated via defining the descriptive functions $f_l(\cdot)$ and the comparative functions $h_l(\cdot,\cdot)$.

In general, the problem of defining networks is difficult when it is not obvious what the relationships between nodes should be. This leads to ad-hoc network generation approaches which can be hard to justify and replicate. In response, functional network generation simplified the problem by requiring only the specification of two functions, identifying at least one benefit of this approach. Definitions for the two functions arise as answers to the following questions:

- **Descriptive**: What is important to the situation under study that can be quantified using the data that we have? (For example, in a military scenario, the military might of each country is of interest and can be put together using available statistics and subject matter expertise.)
- **Comparative**: Given the descriptive values for the quantities of interest what is a reasonable way to compare and contrast them? (For example, this can be as simple as differences and ratios or be made more complicated by incorporating multiple descriptive quantities.)

In response, the following descriptive functions (based on specific elements of the data sources previously introduced) were developed to explore initial escalation scenarios:

- **Enable Capability** = (Command and Control) + 0.5(Cyber Capabilities) + 0.5(Intelligence Capabilities) + 0.75(Air Denial Capabilities) + 0.75(Air Warfare: Enablers)
- **Strategic Capability** = (Ballistic Missile Subs + ICBMs) * (0.75(Command and Control) + 0.5(Area Denial Capabilities))
- **Land Warfare Strike Capacity** = 0.25(Maneuver) + 0.25(Firepower) + 0.75(Ground Based Missiles)
- **Maritime Warfare Strike Capacity** =[0.5(Firepower) +(Sea Control) + 0.5(Sea Denial)] * [0.5(Long Range Force Projection) + 0.5 (Area Denial)]
- **Air Warfare Strike Capacity** = 0.75(Air Warfare: Fighters) * [0.75(Air Warfare: Enablers) + 0.5(Area Denial)]

(**NOTE**: The weightings in these functions were determined through subject matter expert judgement. The weightings, however, were adjusted during the analysis phase of the project to explore sensitivity of the network to metric weights, and future analysis could continue performing sensitivity analysis on these weightings. This could be beneficial not only in improving analytical rigor, but also in exploring how metric weights might vary across countries and across scenarios.)

3.1. Escalation Scenario

The escalation scenarios developed for this project provided opportunities to explore the multilayer network and the concept of escalation in an integrated deterrence context. Three scenarios were selected and developed to consider how realistic crisis triggers might lead to misperceptions and unintended escalation, as countries seek to respond to each other's actions across domains. While the scenarios were relatively simplistic in nature, they provided opportunities to leverage the network and available data to explore the utility of using a multilayer network to better understand escalation in a complex, integrated environment. The scenarios varied in scope and focus to explore different aspects of integrated deterrence and escalation.

Each scenario captures 4 stages of analysis, as shown in Figure 3. Generic Escalation Scenario Stages. The first stage is the "Initial State," where network metrics capture the original structure (including edge weights) of the network. Next is the trigger event, or the "First Action," where one actor in the scenario performs some action that represents changes in network metrics. The third stage is a "Response" step, where the second actor responds to the trigger event. Here, two options are explored. First is an in-kind retaliatory action – "tit-for-tat." Second is an action to restore what was lost, attempting to regain the actor's capabilities to the levels seen in the "Initial State." The fourth stage of analysis is another "Response" stage, where the first actor responds to the second actor's actions. Again, the actions explored include a "tit-for-tat" response and a capability

restoration option. Actions at each stage of analysis represent opportunities for additional changes in network metrics.

From the three developed scenarios, one was examined in initial analysis using the developed multilayer network. In this scenario, the triggering event occurs when Red uses an anti-satellite weapon to destroy one of Blue's satellites. Additional detail on this scenario is described below, while figures capturing the other two scenarios can be found in Appendix A.

For simplicity in analyzing the scenario, two potential responses from Blue were explored. First, Blue could respond to Red's attack by destroying one of Red's satellites in retaliation. This might fit the traditional idea of a "tit-for-tat" response. Alternatively, Blue could respond by seeking to restore the capability that was lost from the satellite's destruction. In the scenario, the Blue satellite that was destroyed performs intelligence, surveillance, and reconnaissance (ISR) functions, so Blue's response could be to restore ISR capabilities by disabling Red's air defense systems and sending ISR aircraft into the region. Each of these options represents a branch in the scenario space. Red then similarly responds in kind or by restoring capabilities to either of Blue's potential actions. This leads to four total branches or paths.

We label the fours paths from left to right at the bottom of Figure 3, A, B, C and D and steps along the path, corresponding to the initial by 1, 2, 3 and 4. Below are the scripts for each path.

- Path A: Both Blue and Red maintain status quo by responding only in kind
    1. The initial state of the world.
    2. Red destroys Blue's satellite causing a decrease in Blue's command and control and area denial capabilities.
    3. Blue performs a tit-for-tat response by targeting Red's satellite and reducing their command and control capabilities.
    4. Red destroys another of Blue's satellites causing a decrease in Blue's command and control and area denial capabilities.
- Path B: Blue responds with a tit-for-tat action followed by Red increasing pressure.
    1. The initial state of the world.
    2. Red destroys Blue's satellite causing a decrease in Blue's command and control and area denial capabilities.
    3. Blue performs a tit-for-tat response by targeting Red's satellite and reducing their command and control capabilities.
    4. Red targets Blue's satellites and scrambles fighters to reduce effectiveness of Blue and Green air warfare capacity and doubly reducing Blue area denial and command and control.
- Path C: Blue responds with an escalatory action followed by Red pursuing a tit-for-tat reaction.
    1. The initial state of the world.
    2. Red destroys Blue's satellite causing a decrease in Blue's command and control and area denial capabilities.

3. Blue destroys Red's satellite reducing Red's ISR capabilities leading to reduction of Red area denial and command and control capabilities. In addition, Blue sends fighter jets to the affected area, reducing Red's fighters and enablers, command and control and area denial.
4. Red destroys another of Blue's satellites causing a decrease in Blue's command and control and area denial capabilities. tit-for-tat response to Blue's escalatory response to Red's initial action, doubly reducing Blue's area denial and command and control, as well as reducing Blue's air warfare capabilities

- Path D: Blue and Red both take aggressive courses of action.
  1. The initial state of the world.
  2. Red destroys Blue's satellite causing a decrease in Blue's command and control and area denial capabilities.
  3. Blue destroys Red's satellite reducing Red's ISR capabilities leading to reduction of Red area denial and command and control capabilities. In addition, Blue sends fighter jets to the affected area, reducing Red's fighters and enablers, command and control and area denial.
  4. Escalatory response to Blue's escalatory response to Red's initial action. Reduce Blue's area denial and command and control three times and reduce Blue and Green air warfare.

Note that all reductions were a constant 50% reduction applied to the prior state.

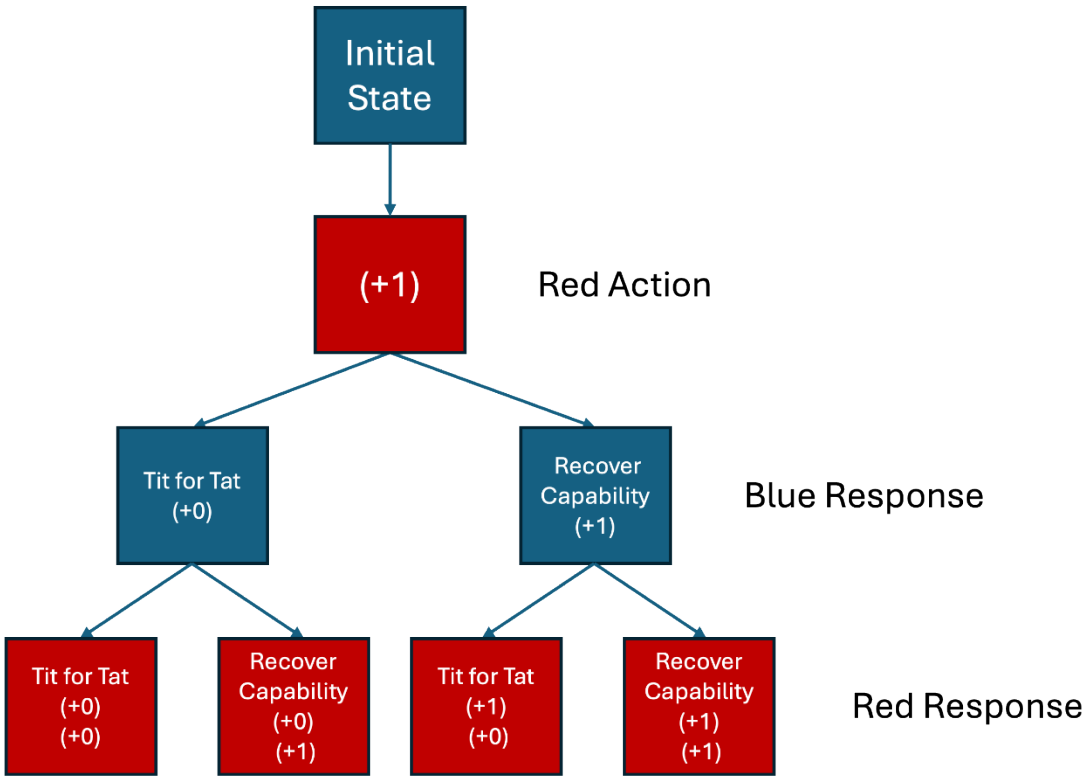


Figure 3. Generic Escalation Scenario Stages

3.2. Scenario Results

Multilayer networks were created for each step of each branch in the state tree shown in Figure 3. Networks were created using the functional edge generation technique described above. Edges were generated by taking differences between node values. The figures below show the paths for Blue, Green and Red for two Asia Power Index data values (e.g., area denial and command and control) and four of the of functional values (e.g., strategic capability, enable capability, and air and maritime strike capacity).

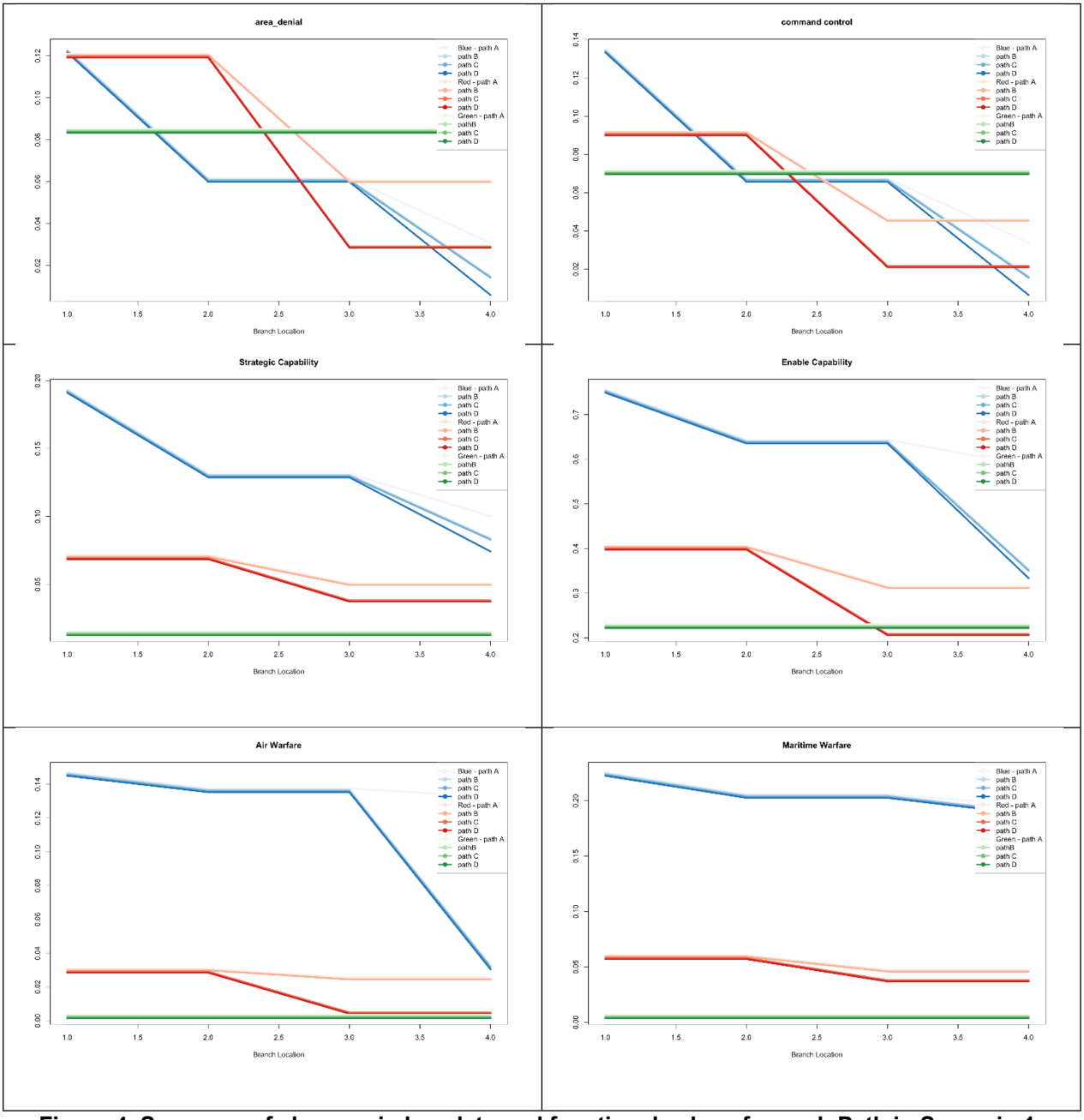


Figure 4. Summary of changes in key data and functional values for each Path in Scenario 1

In addition to tracking node specific statistics and function values we also calculated multilayer network metrics over each of the states.

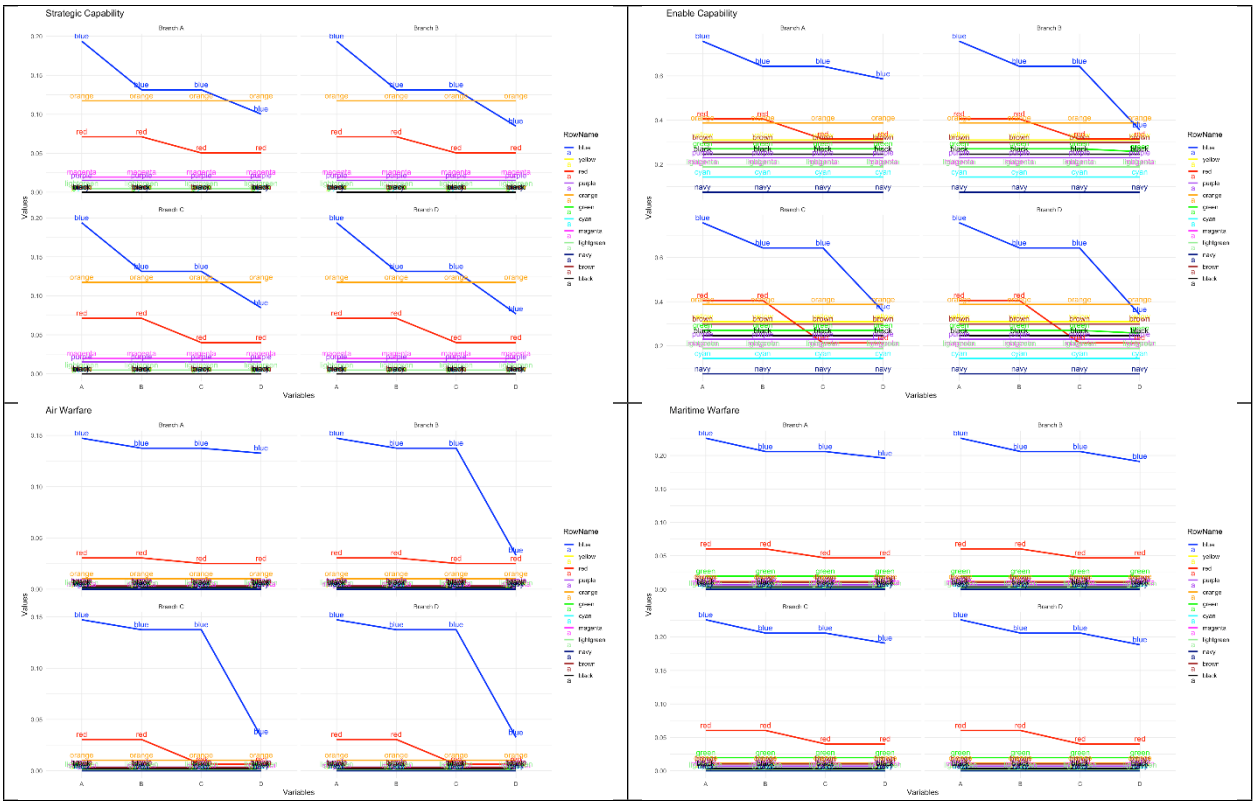


Figure 5. Summary of changes in representative multilayer network metrics calculates for each Path in Scenario 1

The basic results of the scenario demonstrate that the integrated deterrence MLN model can represent how functional capabilities will be impacted during a conflict, and that connections between functional categories are able to represent second and third order effects. For example, the MLN was able to represent how an attack by Red on a satellite would directly reduce Blue command and control and enabling capabilities. The reductions of these values in turn reduced Blue air and maritime warfare capabilities. This level of interaction between states in the model is critical to demonstrating that an MLN model can model a conflict at different levels of specificity.

Comparing the results for the different scenario paths reinforces the utility of the MLN model for understanding varying conflict scenarios. Path A, where both Red and Blue choose a tit-for-tat strategy, shows the smallest reductions of capabilities across all values. This is the expected result, as fewer capabilities were directly impacted in this scenario path. Path D demonstrates the other end of the spectrum with the greatest reductions of capabilities across most values. Again, this as expected considering both Bule and Red took more aggressive actions to restore lost capabilities at each branch. Paths B and C result in very similar values for the four branches but vary the other paths. For air and maritime warfare values, paths B and C have the same value as Path D. In contrast, values for Area Denial, Command and Control, Enable Capabilities, and Strategic Capabilities for Path B and C values diverge from Path D at branch 4. This intuitively matches the scenario description as the level of aggression is greater for Path D than Path B or C.

Turning to network metrics, the most meaning metric to examine is PageRank. PageRank was originally developed by Google to rank web pages. It measures the importance

of nodes based on the idea that connections from important nodes contribute more weight than connections from unimportant nodes. PageRank is a centrality measure that orders nodes based on how connected they are to other important nodes. The results indicate that for most of the scenario Blue PageRank score is highest. Yet, this changes as a result of the actions in Brach 4. The overall loss of capabilities from both Blue and Red result in a decrease of their PageRank scores, ultimately resulting in another country, Orange, moving to have the highest PageRank value. This has interesting implications for diplomatic and economic layers where states may choose to reorient their relationships in light of a perceived weakness from states are a conflict.

3.3. Robustness Checks

Robustness of Results to Changes in Function Values

We repeated the experiments described above with the following updates to the functions.

Variation 1: Updated area denial weighting in air and maritime warfare functions from 0.5 to 0.75

Variation 2: Updated fighters weighting to one in air warfare function.

Variation 3: Updated enablers to one in enable and air warfare functions.

Variation 4: Updated reduction values within steps, including:

- Red Action 1 and Blue's tit-for-tat response (+0): change reduction of area denial and command and control to 25%
- In Blue's aggressive response change reduction of area denial and command and control to 25%. Reduce Red Air warfare: enable = 20%, fighter = 10%. Keep reduction of command and control and area denial at 50%
- Branch B: keep reduction of Blue's area denial and command and control to 50%. Reduce Blue Air warfare: enable = 10%, fighter = 5%. Reduce Green air warfare: enable & fighter = 50%

The robustness checks were performed for two purposes. First, as noted above the primary experiment used the simplifying assumption that all reductions would decrease capabilities by 50%. This figure was arbitrary, as there is no practical reason to assume that a single attack would have such a large reduction of capability, or that the reduction would be consistent across all the functional categories being assessed. Second, varying functional weights also allowed us to detect if changes to any single variable would produce significant shifts in the results.

Overall, results from the robustness checks demonstrated the stability of the MLN model to different functional weights. Variations 1-3 showed that functional weight changes provided small changes to the final values for the functional categories, they did not ultimately alter any of the rankings of Paths A-D in terms of final values. Variation 4 differs from the previous approach by not applying a uniform reduction of capabilities across all states. Instead, it calculates the reduction based on the proportion of Blue and Red aircraft in relation to a 50% reduction in Green aircraft. This method aims to create a more realistic scenario, where the number of destroyed aircraft reflects the overall size of a country's air warfare capability. While the results from this scenario show a less dramatic decrease in Blue and Red's values, the overall findings do not change.

Table 1. Summary of multilayer network air warfare parameter changes for sensitivity and robustness checks

Country	Branch	1	2	3	4	1	2	3	4
Blue	A	0.16	0.14	0.14	0.14	0.20	0.18	0.18	0.18
	B	0.16	0.14	0.14	0.03	0.18	0.18	0.18	0.04
	C	0.16	0.14	0.14	0.03	0.18	0.18	0.18	0.04
	D	0.16	0.14	0.14	0.03	0.18	0.18	0.18	0.04
Red	A	0.04	0.04	0.03	0.03	0.04	0.04	0.03	0.03
	B	0.04	0.04	0.03	0.03	0.04	0.04	0.03	0.03
	C	0.04	0.04	0.01	0.01	0.04	0.04	0.01	0.01
	D	0.04	0.04	0.01	0.01	0.04	0.04	0.01	0.01
Blue	A	0.10	0.09	0.09	0.09	0.16	0.15	0.15	0.14
	B	0.10	0.09	0.09	0.02	0.16	0.15	0.15	0.10
	C	0.10	0.09	0.09	0.02	0.16	0.15	0.15	0.10
	D	0.10	0.09	0.09	0.02	0.16	0.15	0.15	0.10
Red	A	0.02	0.02	0.02	0.02	0.04	0.04	0.03	0.03
	B	0.02	0.02	0.02	0.02	0.04	0.04	0.03	0.03
	C	0.02	0.02	0.00	0.00	0.04	0.04	0.02	0.02
	D	0.02	0.02	0.00	0.00	0.04	0.04	0.02	0.02

NOTE: Air warfare function values for Red and Blue for each of the variations. Green corresponds to the first variation, blue for the second, yellow for the third and orange for the fourth. Changes in initial value are due to changes in the underlying functions.

Table 2. Summary of multilayer network maritime warfare parameter changes for sensitivity and robustness checks

Country	Branch	1	2	3	4	1	2	3	4
Blue	A	0.25	0.22	0.22	0.20	0.23	0.21	0.21	0.20
	B	0.25	0.22	0.22	0.19	0.23	0.21	0.21	0.19
	C	0.25	0.22	0.22	0.19	0.23	0.21	0.21	0.19
	D	0.25	0.22	0.22	0.19	0.23	0.21	0.21	0.19
Red	A	0.07	0.07	0.05	0.05	0.06	0.06	0.05	0.05
	B	0.07	0.07	0.05	0.05	0.06	0.06	0.05	0.05
	C	0.07	0.07	0.04	0.04	0.06	0.06	0.04	0.04
	D	0.07	0.07	0.04	0.04	0.06	0.06	0.04	0.04
Blue	A	0.23	0.21	0.21	0.20	0.25	0.23	0.23	0.21
	B	0.23	0.21	0.21	0.19	0.25	0.23	0.23	0.21
	C	0.23	0.21	0.21	0.19	0.25	0.23	0.23	0.21
	D	0.23	0.21	0.21	0.19	0.25	0.23	0.23	0.21
Red	A	0.06	0.06	0.05	0.05	0.07	0.07	0.06	0.06
	B	0.06	0.06	0.05	0.05	0.07	0.07	0.06	0.06
	C	0.06	0.06	0.04	0.04	0.07	0.07	0.06	0.06
	D	0.06	0.06	0.04	0.04	0.07	0.07	0.06	0.06

Table 3. Summary of multilayer network enable capability parameter changes for sensitivity and robustness checks

Country	Branch	1	2	3	4	1	2	3	4
Blue	A	0.76	0.64	0.64	0.59	0.76	0.64	0.64	0.59
	B	0.76	0.64	0.64	0.36	0.76	0.64	0.64	0.36
	C	0.76	0.64	0.64	0.36	0.76	0.64	0.64	0.36
	D	0.76	0.64	0.64	0.34	0.76	0.64	0.64	0.34
Red	A	0.41	0.41	0.31	0.31	0.41	0.41	0.31	0.31
	B	0.41	0.41	0.31	0.31	0.41	0.41	0.31	0.31
	C	0.41	0.41	0.21	0.21	0.41	0.41	0.21	0.21
	D	0.41	0.41	0.21	0.21	0.41	0.41	0.21	0.21
Blue	A	0.62	0.51	0.51	0.45	0.76	0.70	0.70	0.61
	B	0.62	0.51	0.51	0.29	0.76	0.70	0.70	0.57
	C	0.62	0.51	0.51	0.29	0.76	0.70	0.70	0.57
	D	0.62	0.51	0.51	0.27	0.76	0.70	0.70	0.57
Red	A	0.37	0.37	0.28	0.28	0.41	0.41	0.36	0.36
	B	0.37	0.37	0.28	0.28	0.41	0.41	0.36	0.36
	C	0.37	0.37	0.20	0.20	0.41	0.41	0.35	0.35
	D	0.37	0.37	0.20	0.20	0.41	0.41	0.35	0.35

Table 4. Summary of multilayer network strategic capability parameter changes for sensitivity and robustness checks

Country	Branch	1	2	3	4	1	2	3	4
Blue	A	0.19	0.13	0.13	0.10	0.19	0.13	0.13	0.10
	B	0.19	0.13	0.13	0.08	0.19	0.13	0.13	0.08
	C	0.19	0.13	0.13	0.08	0.19	0.13	0.13	0.08
	D	0.19	0.13	0.13	0.08	0.19	0.13	0.13	0.08
Red	A	0.07	0.07	0.05	0.05	0.07	0.07	0.05	0.05
	B	0.07	0.07	0.05	0.05	0.07	0.07	0.05	0.05
	C	0.07	0.07	0.04	0.04	0.07	0.07	0.04	0.04
	D	0.07	0.07	0.04	0.04	0.07	0.07	0.04	0.04
Blue	A	0.19	0.13	0.13	0.10	0.19	0.16	0.16	0.12
	B	0.19	0.13	0.13	0.08	0.19	0.16	0.16	0.12
	C	0.19	0.13	0.13	0.08	0.19	0.16	0.16	0.12
	D	0.19	0.13	0.13	0.08	0.19	0.16	0.16	0.12
Red	A	0.07	0.07	0.05	0.05	0.07	0.07	0.06	0.06
	B	0.07	0.07	0.05	0.05	0.07	0.07	0.06	0.06
	C	0.07	0.07	0.04	0.04	0.07	0.07	0.06	0.06
	D	0.07	0.07	0.04	0.04	0.07	0.07	0.06	0.06

4. ANALYSIS

One of the fundamental challenges identified from the cross-domain deterrence literature is the difficulty of predicting how movement of a conflict from one domain to another will be perceived by an adversary. Will such a move have a clear deterrent effect or does the crossing of domain boundaries create unanticipated escalatory pressures that could undermine deterrence?

The initial experiment described in Section 3 addressed this question by examining if either Red or Blue had a dominant strategy in the scenario which could indicate whether or not a more aggressive conventional military response to an attack on an asset in space (a cross-domain response) is advantageous. Yet, the overall preference ordering for both Red and Blue are $A \geq B > C \geq D$. This suggests that there is an indication—albeit weak—that a tit-for-tat strategy is dominant in this scenario. However, it is important to note important caveats that exist. First, there is no a priori reason to assume that a state would base decisions to escalate solely on the relative rankings of its own possible outcomes. Several other metrics are possible. First, a state may choose to focus attention on one or two functional capabilities, rather than the full set. Second, a state may choose to focus on its relative outcome to its adversary. Taken together, this could create a situation where a larger loss in a single functional category creates pressures for a more aggressive response. Third, rather than using the final value a state could set a predefined threshold for a specific capability. For example, the loss of 75% of area denial capabilities would cross the line for a nuclear response. Finally, the preference ordering presumes perfect information of how an adversary may respond to an attack.

This last notion gets at a core issue of whether both sides of a conflict will view the same action similarly. For example, for Blue the "restore capability" option of sending aircraft to regain the intelligence, surveillance, and reconnaissance (ISR) capability lost from the destruction of the satellite internally could be seen as a proportional response to maintain the status quo of military capabilities. But to Red, the same action could be seem as escalatory because to regain ISR capability Blue is required to attack Red aircraft and other assets. Thus how "escalatory" an action is interpreted is as much based on the perception of the attacked country as the intentions of attacker. Such misperceptions are challenging enough even within a conventional conflict, as demonstrated in this scenario; but become even more complex when considering how it might be applied in a multi-domain context. Consider the hypothetical situation where a state does not have a symmetrical (e.g. a proportional response within the same domain) way of responding to an adversary action.

While the MLN model cannot answer questions of human decision making, it does indicate why a state may miscalculate. A state may believe its planned action is non-escalatory, resulting in a more favorable outcome (Path A,B) but in reality may be choosing an action that results in a worst payoff (Path C,D). Furthermore, while not presented in this scenario, there is the additional complexity of different time scales across domains. Contemplating an economic or diplomatic response to a military action could be less attractive to a state because the time scale for realizing an economic pressure or building a diplomatic pressure may take too long to be seen as an effective deterrent response. This temporal difference was a significant challenge during the MLN model development, as there are few places where economic or diplomatic responses can feedback into the military domain on a relevant timescale. This leads us to the interesting finding that integrated deterrence may not be well equipped to respond during a crisis. This said, preparing the battlespace, by developing capabilities, plans, and coordination with allies could mitigate some of these challenges and improve general deterrence.

A second question this project sought to address is whether there is a difference in the way escalation progresses in traditional nuclear deterrence models from an integrated deterrence framework? Here we find that traditional theories of escalation still apply to integrated deterrence. Issues of relative capabilities, strategic stability should still hold within specific domains. However, as previously noted perceptions of proportionality and escalation become more complex at the edges of domains. The lack of established norms in the cyber, space, and gray-zone domains will continue to pose challenges. Additionally, the results of the scenario indicate that traditional deterrence theories underestimate the importance of enabling capabilities in understanding escalation. Modern offense capabilities rely on a large support architecture of enabling capabilities to function. Adversary actions that degrade or eliminate these enabling capabilities, such as the destruction of a satellite, could create significant escalatory pressure if militaries seek to restore those functions. This dynamic is potentially made worse if enabling and command and control functions are shared by conventional and nuclear capabilities.

5. CONCLUSIONS, INSIGHTS, AND IMPLICATIONS

This project sought new technical understanding of potential cross-domain conflict escalation pathways to provide a rigorous and structured approach for evaluating—and comparing the relative risks of integrated deterrence. To accomplish this, the research team explored the efficacy of using multilayer network models to represent across different domains and actions. Operationalizing the complex and often ill-defined nature of integrated deterrence proved challenging. Nevertheless, the research team successfully developed an MLN model and exemplar escalation scenarios to explore how actions progress through and across different domains.

5.1. Insights

5.1.1. Insights on a "Theory" of Integrated Deterrence

- A tit-for-tat strategy to control escalation appears as a promising approach to control escalation risks within integrated deterrence. This will require further study to explore if this initial finding holds across other domains. For example, developing a set of cross-domain options in cases for presumed symmetric responses would be valuable.
- Enabling capabilities are a lynchpin for managing escalation risks. While often considered as an important piece of conventional military operations, enabling capabilities have normally been ignored as part of nuclear deterrence and escalation theories. This should change when considering integrated deterrence. Enabling capabilities—in military, economic, and diplomatic—domains will be crucial for the US to take economic actions, access theaters for military strikes and/or defend US forces and territory and maintain diplomatic links. The importance of enabling capabilities for US integrated deterrence also makes them centers of gravity for adversaries to target.
- Time scales of actions across economic, military, and military elements of integrated deterrence vary widely. This will make cross-domain responses in conflict difficult. Scenarios tend to be short-term, but cross-domain escalation and integrated deterrence require longer-term thinking. Often, escalation across domains may be somewhat subjective and prone to messaging. The connections between Diplomatic layer and Economic layer are typically limited. People can arbitrarily decide to move across layers for messaging, but there may not be a specific logic that leads from one to the next. These two features lead to the conclusion that integrated deterrence should be thought of more as shaping the deterrence environment and general deterrence to reinforce desired perceptions in other countries, rather than using cross-domain deterrence for crisis deterrence and conflict escalation scenarios.
- Perception of the adversary is key for understanding and effective modelling deterrence scenarios. While this has always been true for traditional deterrence, it is compounded in cross-domain deterrence scenarios. Actions intended to restore deterrence can easily be viewed as escalatory by an adversary. This is compounded when the capability one is trying to restore requires action in a different domain (e.g. using aircraft to restore ISR capabilities lost from an attack on a satellite). Further the dearth of norms in emerging domains of cyber, space, and the grey zone could lead to additional misperceptions.

5.1.2. Insights on the Applicability of MLNs for Deterrence and Escalation

- This research process has shown the utility of MLN models for understanding complex dynamics within cross-domain deterrence. Specifically, the ability of MLN models to explicitly draw functional relationships across nodes, allowing greater understanding of first and second order impacts of actions. Additionally, MLN models are better able to represent more state actors than game-theoretic approaches. These features are critical for understanding the complex relationships within domains and how that interacts with other state actions
- The detail available within MLN models help demonstrate the connections between specific technologies and political/military dynamics. Each node can accommodate considerate amounts of data which allowed for the creation of functional edges. These edges are crucial for representing the multiple factors at work in a single interstate interaction. This ability allows for a more nuanced understanding of how a specific technology could alter these functional relationships, and in turn impact overall political/military dynamics.
- Data availability for all network layers is a central challenge (at least open source data). While the importance of quality data is by no means novel to MLNs, it remains an important role in the type and depth of analysis for cross-domain deterrence questions. As by its nature, cross-domain MLNs need to represent interactions across different domains, they must also collect data for each network layer. The challenge lies in finding data with sufficient specificity to enable meaningful network connections. While the corpus of data collected for this research effort was sufficient to build a notional model of military, economic, and diplomatic layers, the operationalization of some variables colored the type of analysis possible. Moving from a notional model to "real-world" would require large data collection efforts. This could be a serious limiting factor for future use of MLN models for integrated deterrence.

5.2. Implications

The insights from this research effort represent an initial attempt at providing a conceptual, scientific, and analytical foundation for supporting broader U.S. deterrence strategic thinking on cross-domain deterrence. We believe that the development of such a model demonstrates Sandia's position at the forefront of multilayer network analysis for U.S. national security goals and demonstrates the Labs' multidisciplinary capability to meet mission needs in increasingly complex national security environments. Expanding on the current mission need with mission specific scenarios and data, along with paring this model with other Sandia political decision making modelling efforts will place Sandia on the forefront of thinking of cross-domain deterrence, and enable it to support a wide variety of sponsors in the future.

REFERENCES

[1] B. Roberts, The Case for U.S. Nuclear Weapons in the 21st Century, Stanford Univ. Press, 2015.

[2] B. Roberts, "On Theories of Victory, Red and Blue," *Livermore Papers on Global Security*, No.7, June 2020.

[3] U.S. Department of Defense. "Nuclear Posture Review of the United States of America," February 2018, p. 52-53.

[4] U.S. Department of Defense. "National Defense Strategy of the United States of America," October 2022.

[5] M. Mazarr et al., "What Deters and Why: Applying a Framework to Gray Zone Aggression," RAND Corporation, Santa Monica, CA, 2021.

[6] E. Gartzke and J. Lindsay, "Cross-Domain Deterrence: Strategy in an Era of Complexity," presented at the International Studies Association Annual Meeting, Toronto, July 2014, p. 8.

[7] B. Radzinsky, "Setting Priorities for Deterrence Integration: Workshop Summary," *Lawrence Livermore National Laboratory Center for Global Security and Research*, August 2021.

[8] E. Lonergan and J. Schneider, "The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation," *Journal of Cybersecurity*, vol. 9 no. 1, Mar. 2023.

[9] S. Kreps and J. Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-based *Logics*," *Journal of Cybersecurity,* vol. 5 no. 1, 2019.

[10] K. Mallory, *New Challenges in Cross-Domain Deterrence,* Santa Monica, CA, RAND Corporation, April 2018.

[11] T. Sweijs and S. Zilincik, "From Deterrence to Cross Domain Deterrence" in *Cross Domain Deterrence and Hybrid Conflict*, Hague Centre for Strategic Studies, 2019.

[12] T. Sweijs et al., *A Framework for Cross-Domain Strategies Against Hybrid Threats*, HCSS Security, Hague Centre for Strategic Studies, 2021.

[13] R. Hersman, "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review*, vol. 3 no. 3, Autumn 2020.

[14] G. Bianconi, *Multilayer Networks: Structure and Function*, United Kingdom, Oxford Univ. Press, 2018.

[15] R. J. Vince, "Cross-Domain Deterrence Seminar Summary Notes," Proceedings, Livermore, California, Nov. 18-19, 2014. Lawrence Livermore National Laboratory. [Online]. Available: https://cgsr.llnl.gov/sites/cgsr/files/2024-08/SummaryNotes.pdf

[16] H. Kahn, On Escalation: Metaphors and Scenarios. Routledge, 2017.

[17] J. Lo, N. K. Jie, and H. Lo, "Reconstructing the ladder: Towards a more considered escalation model of escalation," *Strategy Bridge*, 2022.

[18] T. Sweijs and S. Zilincik, "From Deterrence to Cross Domain Deterrence," in *Cross Domain Deterrence and Hybrid Conflict*, Hague Centre for Strategic Studies, 2019, pp. 11–18.

[19] E. D. Lonergan and J. Schneider, "The power of beliefs in US cyber strategy: The evolving role of deterrence, norms, and escalation," *Journal of Cybersecurity*, vol. 9, no. 1, 2023.

[20] E. D. Lonergan and S. W. Lonergan, "Cyber operations, accommodative signaling, and the de-escalation of international crises," *Security Studies*, vol. 31, no. 1, pp. 32-64, 2022.

[21] J. Schneider, "The biggest cyber risk in Ukraine? How Russian hacking could threaten nuclear stability," *Foreign Affairs*, 2022.

[22] B. Jensen and B. Valeriano, "What do we know about cyber escalation: Observations from simulations and surveys," *The Atlantic Council Scowcroft Center for Strategy and Security*, 2019.

[23] M. Brecher, "Crisis escalation: Model and findings," *International Political Science Review*, vol. 17, no. 2, pp. 215-230, 1996.

[24] R. Hersman, "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review*, vol. 3, no. 3, pp. 90-109, 2020.

[25] C. A. Hidalgo, A Tale of Two Literatures: An Antidisciplinary Review of Social Networks and Network Science, Unpublished Manuscript, MIT Course MAS.581-Networks, Information and the Evolution of Complex Systems., 2014.

[26] G. Bianconi, Multilayer networks: structure and function, Oxford university press, 2018.

[27] Y. Y. Liu, J. J. Slotine and A. L. Barabasi, "Control centrality and hierarchical structure in complex networks," *Plos one,* vol. 7, no. 9, 2012.

[28] S. Gomez, A. Diaz-Guilera, J. Gomez-Gardenes, C. J. Perez-Vicente, Y. Moreno and A. Arenas, "Diffusion dynamics on multiplex networks," *Physical review letters,* vol. 110, no. 2, 2013.

[29] M. Kivela, "Multilayer Networks," *Journal of Complex Networks,* vol. 2, no. 3, pp. 203-271, 2014.

[30] F. Battiston, V. Nicosia and V. Latora, "Structural measures for multiplex networks," *Physical review. E.,* vol. 89, no. 3, 2014.

[31] J. Gómez-Gardeñes, I. Reinares and A. Arenas, "Evolution of Cooperation in Multiplex Networks," *Scientific Reports,* vol. 2, p. 620, 2012.

[32] Office of the Chairman Joint Chiefs of Staff, The National Military Strategy of the United States of America: A Strategy for Today; a Vision for Tomorrow, 2004.

[33] C. Drewien, "Cross-Domain Deterrence: Presentation to US Air Force Academy," SAND2019-4413PE, 2019.

[34] Joint Chiefs of Staff, Joint Doctrine Note 1-18: Strategy, 2018.

[35] S. Heffington, A. Oler, and D. Tretler, "A National Security Strategy Primer," 2019.

[36] NATO Standardization Office, NATO Standard AJP-01: Allied Joint Doctrine, 2017.

[37] B. Bonin et al., "Global Nuclear Enterprise (GNE) FY 18 System Study Summary," [Unpublished manuscript], 2019.

[38] A. D. Williams *et al.*, "Early results from applying a multilayered network framework to engineer nuclear security systems," in *Proceedings of the Institute of Nuclear Materials Management & ESARDA Joint Virtual Annual Meeting*, 2021.

[39] A.D. Williams et al., "LDRD23-0730: Invoking Multilayer Networks to Develop a Paradigm for Security Science—Summary Report. SAND2023-11049, October 2023.

This page left blank

APPENDIX A. ADDITIONAL ESCALATION SCENARIOS

In addition to the scenario described and analyzed in Section 3 of this report, the following two scenarios were also developed. Scenario 2 examines a situation where microchip exports essential for military applications are sanctioned. Scenario 3 outlines a combined information campaign and cyber attack as the trigger event. While these two scenarios were not analyzed using the multi-layer network, they were used to inform the structure and creation of the network.

Scenario 2 – Microchip Sanctions:

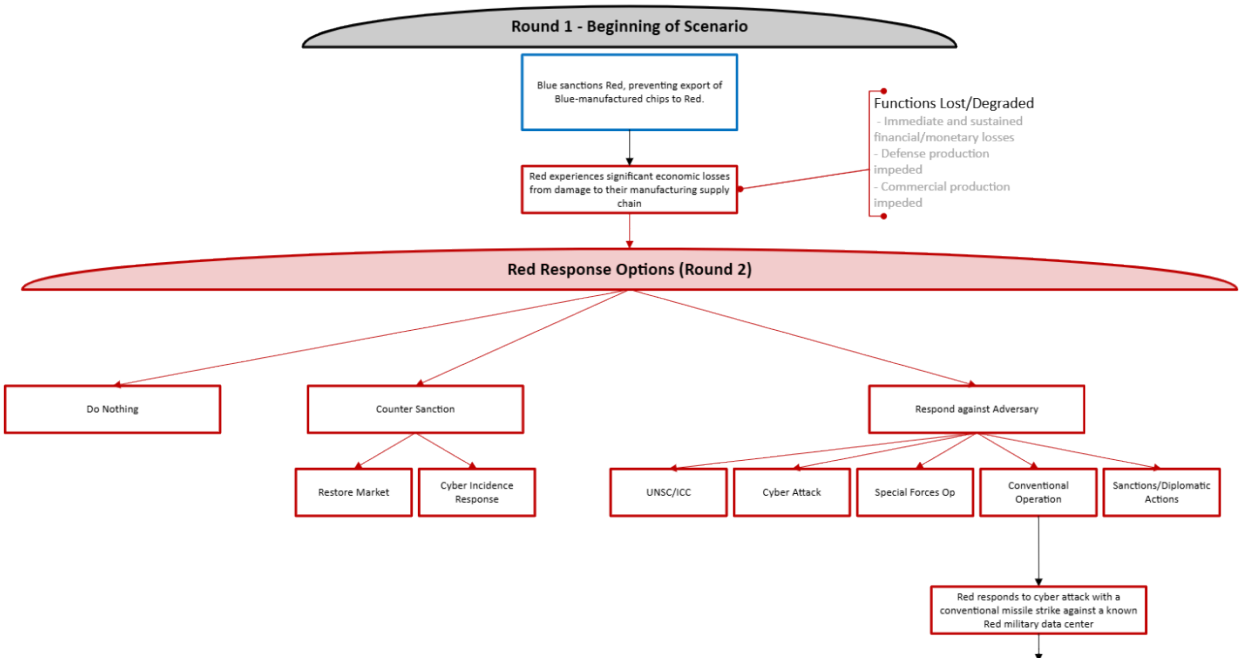


Figure 66. Scenario 2 Rounds 1-2

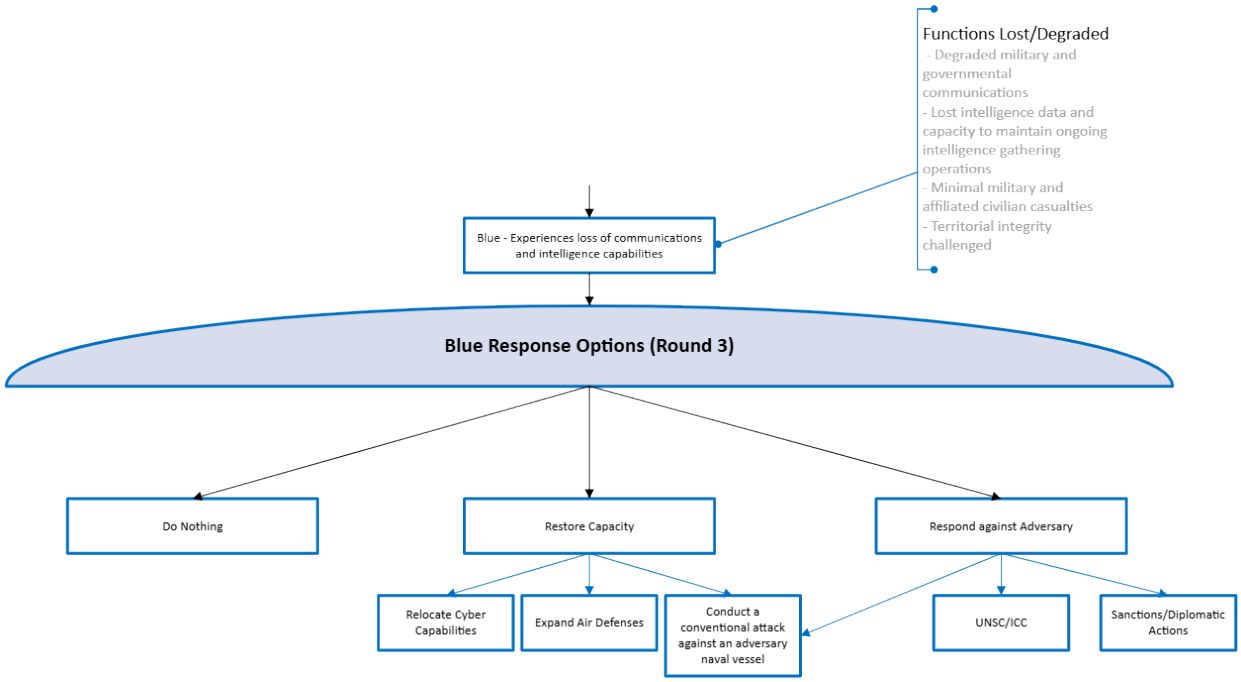


Figure 77. Scenario 2 Round 3

Scenario 3 - Information Campaign and Cyber Operations

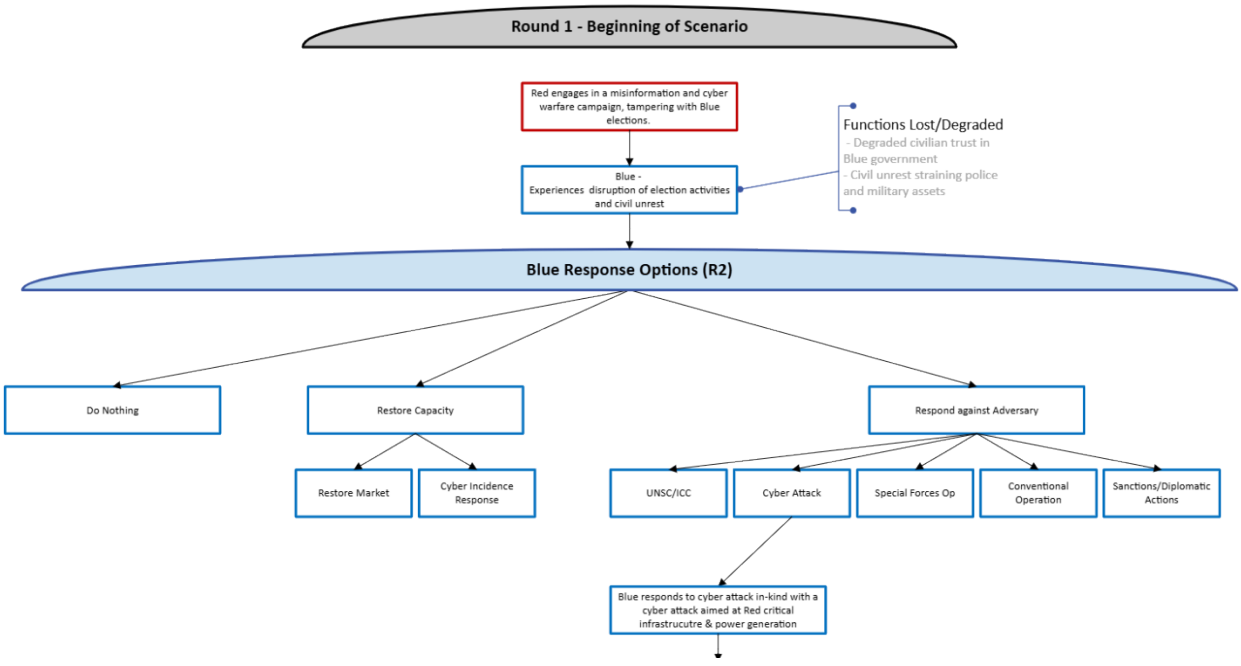


Figure 88. Scenario 3 Rounds 1-2

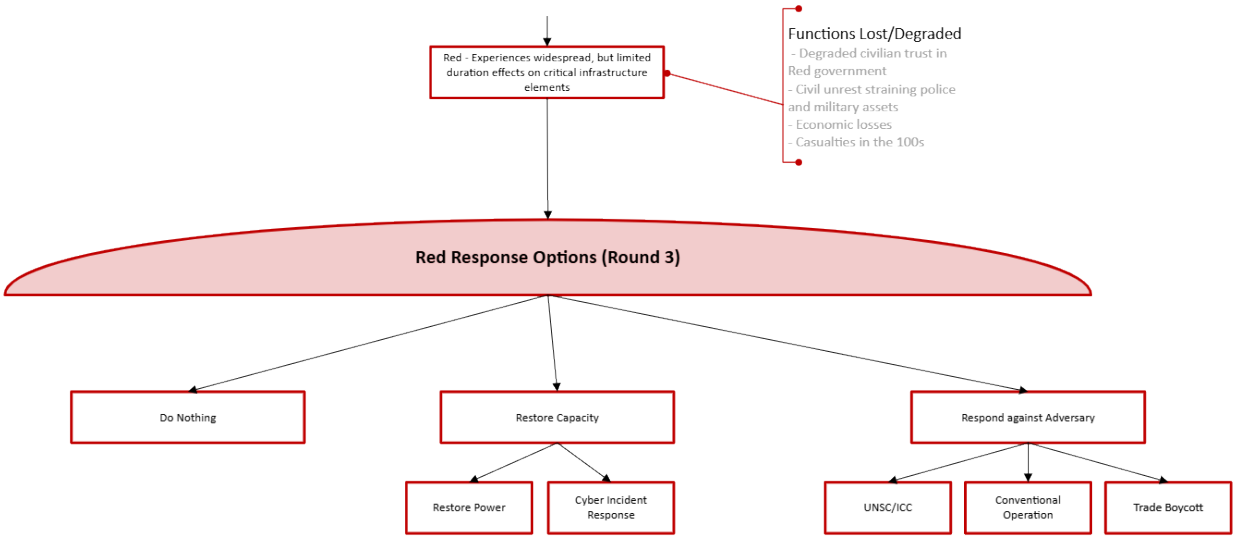


Figure 99. Scenario 3 Round 3

APPENDIX B. ADDITIONAL RESULTS FROM THE MLN

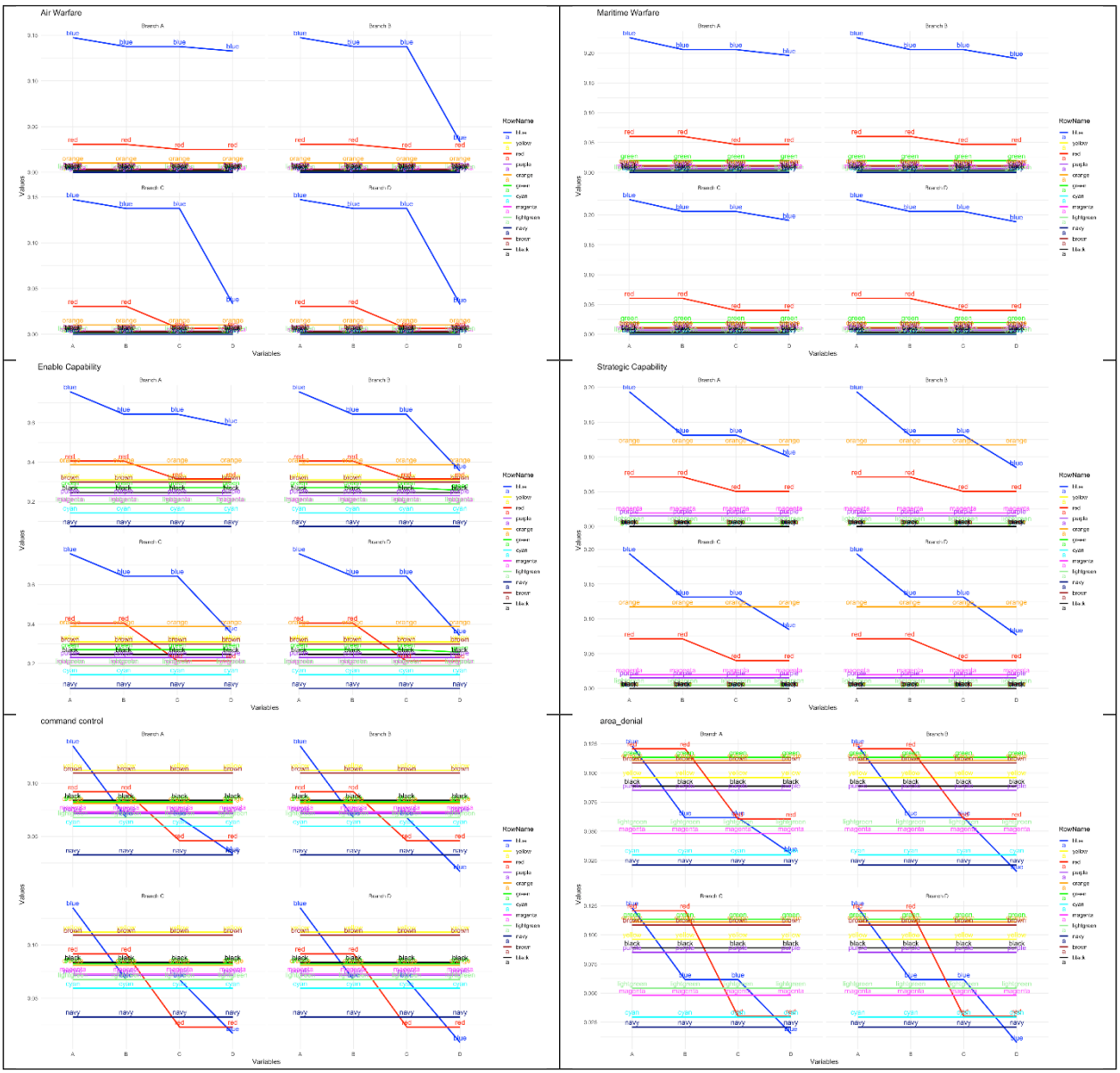
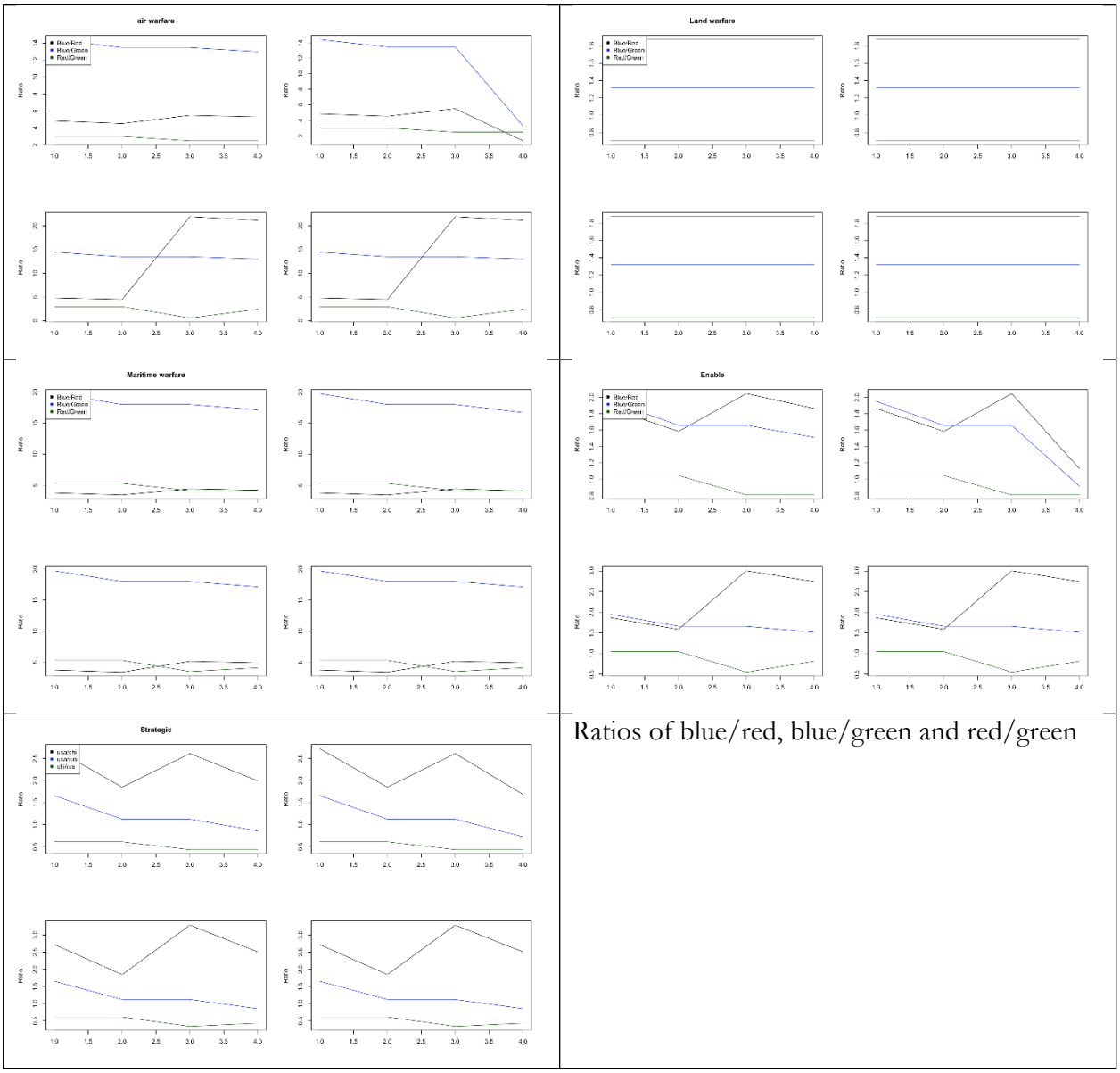
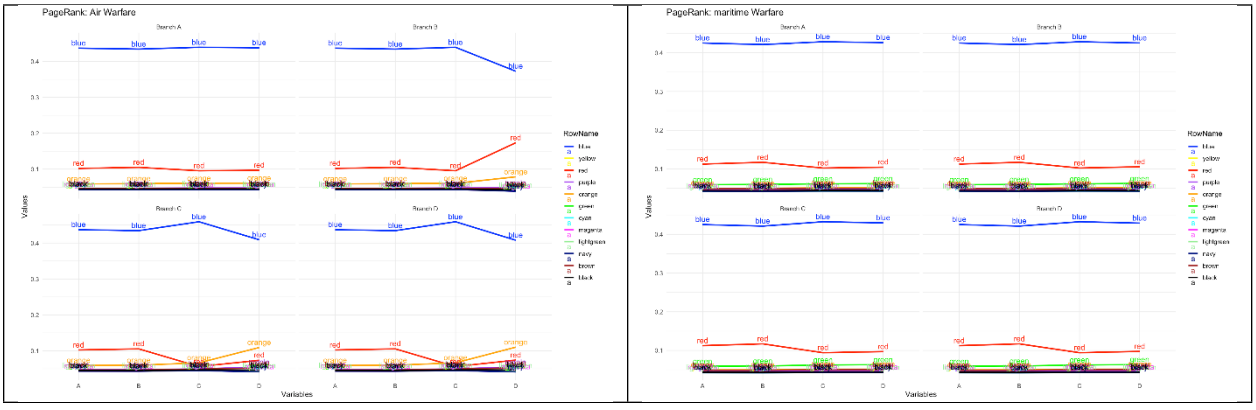


Figure 910. MLN results for All Countries



Ratios of blue/red, blue/green and red/green

Figure 1011. Ratios of Blue/Red, Blue/Green and Red/Green Values



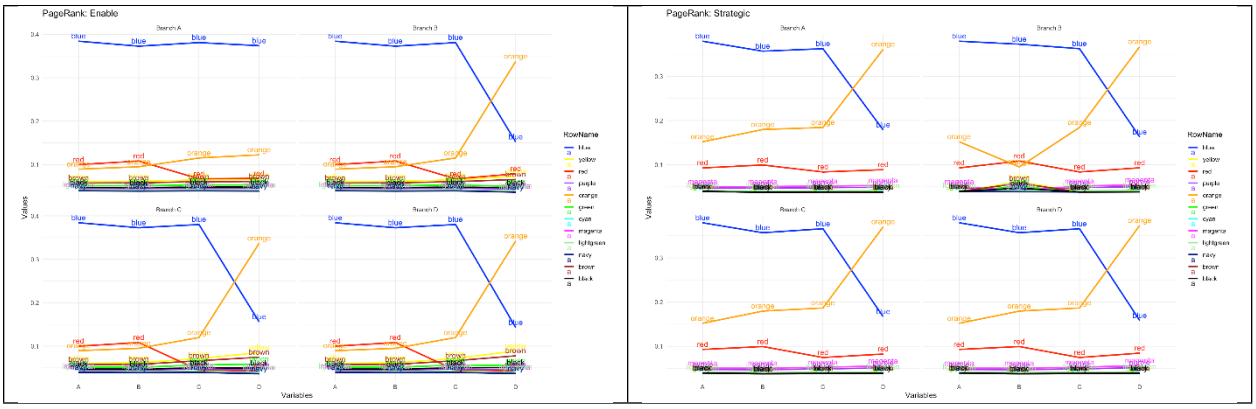


Figure 1112. PageRank Metrics for all Countries in the Scenario

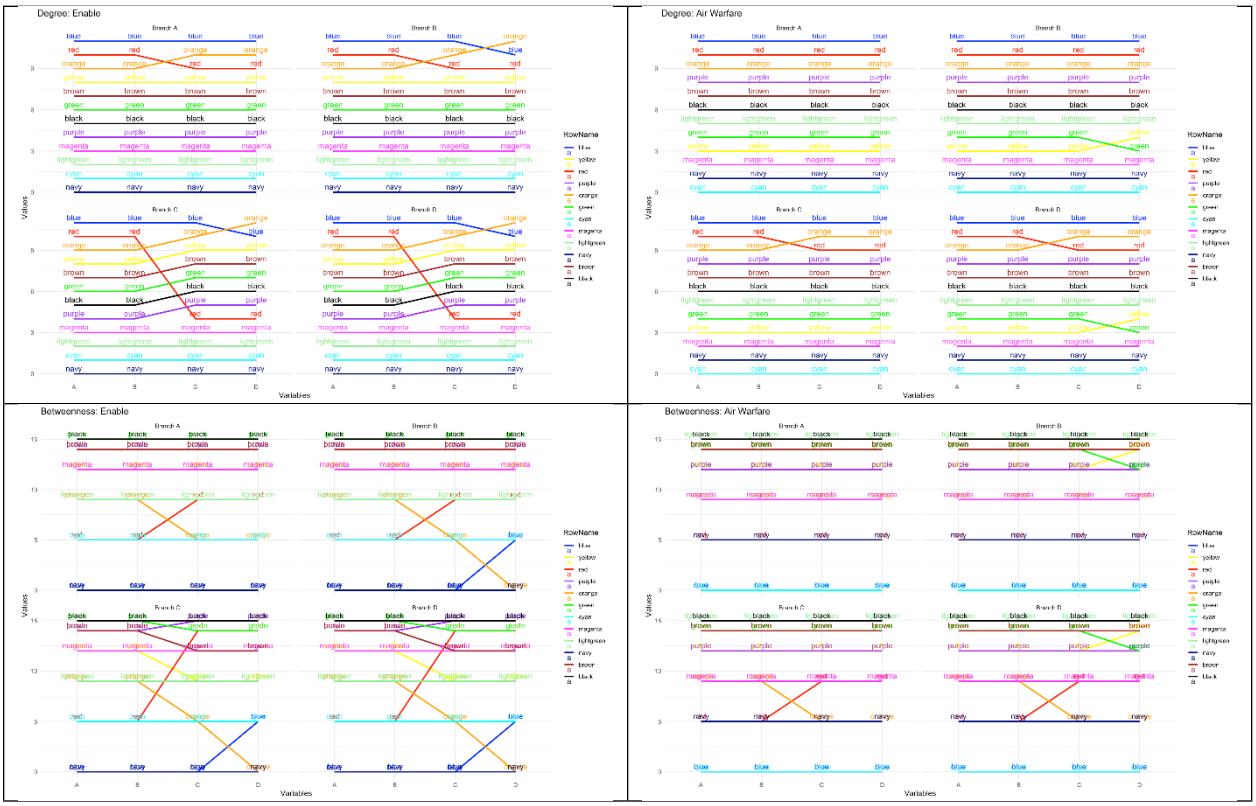


Figure 1213. Other Network Metrics: Degree and Betweenness Centrality

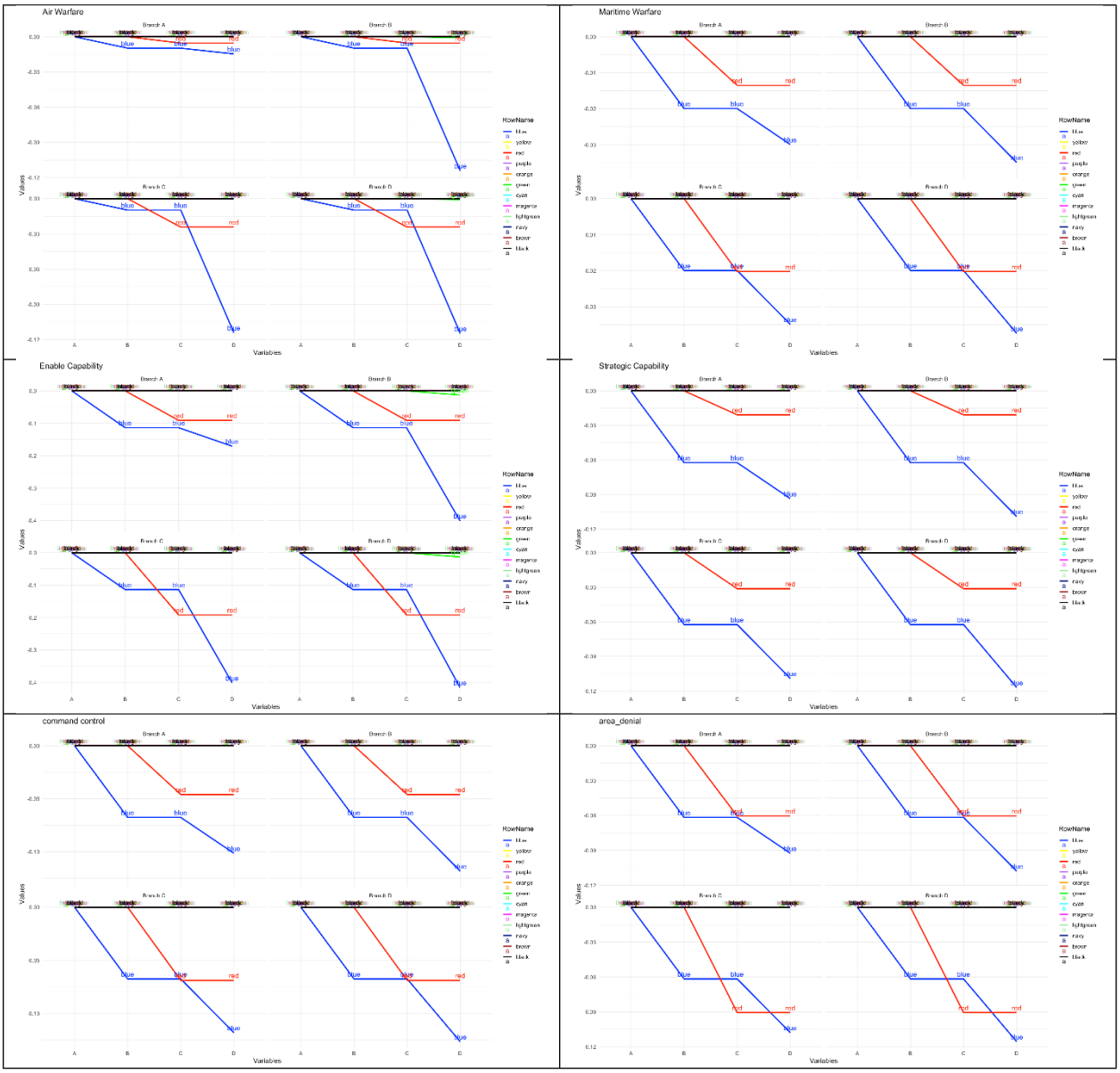


Figure 1214. Other Network Metrics: Metric First Difference

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Amir Mohagheghi	6800	ahmohag@sandia.gov
Adam Williams	6812	adwilli@sandia.gov
Sam Gailliot	6817	sfgaill@sandia.gov
Eric Wallace	6834	eawalla@sandia.gov
Mathias Boggs	8714	mdboggs@sandia.gov
Technical Library	1911	sanddocs@sandia.gov

This page left blank

Sandia National Laboratories

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.