Research Report

KRISTA ROMITA GROCHOLSKI, SCOTT SAVITZ, SYDNEY LITTERER, MONIKA COOPER, CLAY MCKINNEY, ANDREW ZIEBELL

Assessing the Impact of Diverse Intermediate Force Capabilities and Integrating Them into Wargames for the U.S. Department of Defense and NATO

For more information on this publication, visit **www.rand.org/t/RRA1544-1**.

Published by the RAND Corporation, Santa Monica, Calif.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-1031-3

Cover photo: USS New Orleans (LPD 18).

About This Report

Non-lethal weapons (NLWs) include a diverse range of systems, such as acoustic hailing devices, eye-safe laser dazzlers, millimeter-wave emitters that cause a temporary heating sensation, and entangling devices to stop vehicles or vessels. Evaluating the impact of NLWs—whose intent is to limit harm to people and objects—requires a different approach from evaluating most weapons employed by the U.S. Department of Defense (DoD) and the North Atlantic Treaty Organization (NATO) alliance. A prior RAND report (Romita Grocholski et al., 2022) characterized how to measure their impact using a structure called a *logic model* and associated metrics. It also included a series of vignettes that revealed the versatility of these systems.

The Joint Intermediate Force Capabilities Office (JIFCO), which sponsored both that report and this one, oversees NLW efforts for DoD. JIFCO characterizes NLWs as part of a suite of *intermediate force capabilities* (IFCs), alongside electromagnetic warfare, cyber, and information operations. One feature that these IFCs share is that their impact is difficult to measure.

This report updates the prior logic model to reflect current DoD and NATO strategic goals, and also expands on it to encompass all IFCs. Moreover, it presents vignettes and metrics that help to characterize when and how IFCs have an impact. Finally, it characterizes how IFCs can be better integrated into wargaming, as well as associated modeling and simulation, in ways that can facilitate understanding of them and contribute to their integration into operations.

National Security Research Division

This research was sponsored by the Joint Intermediate Force Capabilities Office (JIFCO) and conducted within the Navy and Marine Forces Program of the RAND National Security Research Division (NSRD), which operates the National Defense Research Institute (NDRI), a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise. The research reported here was completed in September 2022 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

For more information on the RAND Navy and Marine Forces Program, see www.rand.org/nsrd/nmf or contact the director (contact information is provided on the webpage).

Acknowledgments

We would like to thank the many people who took the time to share their expertise and insights with us from the following organizations:

- Air Force Research Laboratory
- Army University
- Center for a New American Security
- Center for Army Analysis
- Center for Naval Analyses
- George C. Marshall European Center for Security Studies
- Institute for Defense Analyses
- Joint Staff J8

- Joint Intermediate Force Capabilities Office
- LEC Management
- Marine Corps University
- Naval Postgraduate School
- NATO System Analysis and Studies Research Task Group (SAS-151)
- Office of Net Assessment
- Office of the Secretary of Defense
- U.S. Army Command
- U.S. Naval War College.

We would also like to express our gratitude to the Joint Intermediate Force Capabilities Office (JIFCO) for sponsoring this work. We received valuable guidance and information from our action officer, Susan LeVine, as well as many of her colleagues, including John Nelson, Brian Long, and Eric Duckworth. We also greatly appreciated direction and feedback from Colonel Wendell B. Leimbach, Jr., who heads JIFCO. In addition, Peter Dobias, Sean Havel, and many other members of the NATO System Analysis and Studies Research Task Group (SAS-151) provided thoughtful feedback and guidance. We would also like to thank the unit managers who oversaw this research, Paul DeLuca and Brendan Toland, for their comments and encouragement. Finally, we wish to thank our reviewers, Terrence Kelly and Peter Perla, for helping us to improve the document.

Summary

Background and Purpose

Non-lethal weapons (NLWs) include a highly diverse set of systems, such as acoustic hailing devices, eye-safe laser dazzlers, flash-bang grenades, rubber bullets, millimeter-wave emitters that cause a temporary heating sensation, microwave emitters that shut down electronics, and entangling devices to stop vehicles or vessels. As was documented in a previous RAND report (Romita Grocholski et al., 2022), the U.S. Department of Defense (DoD) can employ NLWs for a range of purposes in a variety of contexts. That report also characterized how NLWs ultimately contributed to DoD-wide strategic goals, using a structure called a *logic model*, and examined the potential usage of NLWs across a range of vignettes, as well as ways of measuring the impact of NLWs. The Joint Intermediate Force Capabilities Office (JIFCO), which sponsored this work and oversees NLW efforts for DoD, characterizes NLWs as part of a suite of *intermediate force capabilities* (IFCs), alongside electromagnetic warfare (EW), cyber, and information operations (IO).[1]

JIFCO asked RAND to build on this prior work in three distinct respects. The first was to update the logic model so that it addressed the strategic goals enumerated in the 2022 National Defense Strategy (NDS). The second was to create a new version of the logic model that would address the needs of the North Atlantic Treaty Organization (NATO), particularly expanding to include all IFCs (NLWs, EW, cyber, and IO) and incorporate NATO strategic goals. The third was to characterize how IFCs could be better integrated into wargames, as well as modeling and simulation (M&S). This report describes the results of these three interrelated efforts.

Methodology

Each part of the analysis entailed a distinct methodology. To revise the DoD-centric logic model to reflect the 2022 NDS, we first extracted the relevant strategic goals from a publicly available fact sheet on the new NDS (DoD, 2022; the full unclassified version of the NDS has not been made publicly available at the time of writing, in early 2022). We then linked these new strategic goals with the outcomes from the original logic model. The development of a NATO-centric IFC logic model required an expansion of the original logic model's scope to include IO, EW, and cyber defense. NATO focuses solely on cyber defense and resilience, therefore references to cyber in this report are to be considered only in the context of defense. We analyzed documents and interviewed subject-matter experts to identify elements of the logic model for these three additional warfare areas, then drew strategic goals from NATO documents. We developed 11 NATO-centric vignettes in order to confirm the utility of the logic model's elements in relating to those vignettes. In addition, we analyzed which elements of the logic model related to one another, and to what degree, while also identifying several metrics for each element of the logic model. Finally, we reviewed documents and conducted interviews to determine how IFCs could be integrated into wargaming and associated M&S.

[1] Electromagnetic warfare is also a significant capability that is used in kinetic/lethal warfare. In the IFC context, we only refer to non-lethal use of this capability.

Updated Strategic Goals for DoD Logic Model on Non-Lethal Weapons

A logic model is a framework that links *inputs* that enable *activities*, whose direct *outputs* contribute to higher-level *outcomes* and ultimate *strategic goals*. All of these items are collectively termed *elements* of the logic model. We extracted a new set of strategic goals for the updated DoD logic model from the publicly available 2022 NDS fact sheet (DoD, 2022). These strategic goals are strengthening alliances and partnerships, improving DoD's competitive advantage, building a more resilient force, defending the homeland, deterring aggression and attacks, and prevailing when necessary. The strategic goals are the only elements that differ from the version of the NLW logic model that was presented in the prior report.

NATO Logic Model, Metrics, and Vignettes for IFCs

There are two key differences between the NATO-centric and DoD-centric versions of these materials. The first is that the NATO version has a broader scope that includes NLWs, IO, EW, and cyber. The second difference is that the logic model's strategic goals are derived from NATO documents, rather than from DoD sources. Figure S.1 shows that the NATO logic model is more voluminous than the DoD-centric version because of the expansion in scope, almost doubling in size (75 elements versus 42 elements). We also characterized the connections between elements in adjacent levels of this logic model, which helped reveal which elements are best linked to NATO's strategic goals.

We identified metrics for each of the new elements in the NATO logic model, totaling 153 metrics for the 31 new elements relating to IO, EW, and cyber. We also developed a series of 11 vignettes to help validate the NATO logic model and to illustrate the contexts of IFC usage. By design, the vignettes collectively entail use of NLWs, IO, EW, and cyber capabilities, and most involve multiple capabilities. They reflect a range of missions, challenges, operational contexts, and geographic regions in which NATO may employ these capabilities.

Integrating IFCs into Wargames and Modeling and Simulation

To identify how IFCs might be integrated into DoD wargames, we interviewed 26 wargamers with a wide range of expertise and reviewed several relevant documents (e.g., Perla, 1990). We also observed a series of wargames run by the NATO System Analysis and Studies Research Task Group (SAS-151). The process of helping to develop and document the NATO IFC wargames also contributed to our analysis.

Conclusions

We found that the NLW logic model that we created for our previous study continues to be robust and relevant: The same set of activities, outputs, and outcomes from that logic model strongly support the strategic goals we derived from both the 2018 and 2022 NDSs. These remain the elements of the logic model that should be focused on when assessing the impacts of NLWs. Notably, the five key outcomes in this logic model were

- competing effectively and demonstrating resolve while managing escalation
- conducting operations in environments that would otherwise be too risky
- avoiding alienation of host-nation populations, forces, and governments

FIGURE S.1
All Elements of the NATO-Centric Logic Model

Inputs

- Communications platforms and media
- Network infrastructure and software
- Integration into warfighting processes
- Domain-specific expertise
- Industrial base
- IFC systems‡
- Concepts of operations (CONOPS) and employment (CONEMP)‡
- Tactics, techniques, and procedures‡
- Doctrine‡
- Training‡
- Sustainment‡
- ISR‡

Activities

- Hail to clarify, demarcate, and warn‡
- Reveal other parties' intent‡
- Affect mobility: Slow, impede, halt, prevent from approaching or leaving, redirect, disperse, impel departure‡
- Compel/tactically deter: Convince others to take or not take specific actions‡
- Temporarily incapacitate personnel‡
- Incapacitate infrastructure/materiel‡
- Disseminate information to inform and persuade
- Expose malign information operations
- Disseminate information to affect adversary perceptions and assessments
- Detect and identify sources of electromagnetic (EM) radiation
- Characterize, locate, and track sources of EM radiation
- Conduct reconnaissance against, exploit, and establish persistent presence in adversary systems to prepare the cyber battlespace
- Defend/protect/remediate NATO front-line systems against EW
- Defend and remediate NATO networks and critical infrastructure (e.g., data backbone) against cyber and EW (includes diagnosis of issues)
- Secure, configure, maintain, and protect existing networks to prevent attacks
- Deceive, distract, disorient, or confuse‡
- Degrade, disrupt, and destroy adversary systems and C^{4}ISR

Outputs

- Affected perceptions, decisionmaking, and behavior of adversary leadership
- Affected perceptions, decisionmaking, and behavior of adversary personnel
- Affected adversary leadership's emotional state, judgement, and will to fight
- Affected adversary personnel's emotional state, judgement, and will to fight
- Avoided effects of adversary manipulation of information to affect perceptions, attitudes, decisions, and behaviors of NATO and partner forces
- Avoided effects of adversary manipulation of information to affect perceptions, decisionmaking, and behavior of populations in NATO members, partner nations, and neutral nations
- Influenced perceptions, decisionmaking, and behavior of populations
- Achieved knowledge of adversary networks
- Created actionable objectives in adversary networks to facilitate their potential disruption/degradation/destruction (potentially prior to conflict)
- Disrupted, degraded, manipulated, and/or destroyed adversary networks
- Minimized disruption, degradation, manipulation, and destruction of networks and systems, as well as recovery time and costs, from EW and/or cyberattack
- Effectively responded to situations despite constraints‡
- Enabled pre-emptive action without appearing to be aggressor‡
- Increased options for engaging targets‡
- Reduced risk of exceeding rules of engagement or Laws of War‡
- Reduced adversary options and imposed costs‡
- Gained time/distance before deciding to take lethal action‡
- Enabled lower-signature clandestine ops‡
- Reduced risk of NATO, partner personnel casualties‡
- Minimized collateral damage and fratricide‡
- Reduced risk to NATO systems or facilities‡
- Gathered intelligence from captured personnel and materiel, as well as from cyber and EW means‡
- Conserved and augmented lethal capabilities‡
- Reduced NATO tactical costs (broadly defined)‡
- Disrupted adversary decision cycle to provide relative advantage to NATO forces and degrade adversary ability to employ forces effectively

Outcomes

- Maintained credibility and legitimacy of NATO and partner forces
- Reduced credibility and legitimacy of adversaries
- Prevented and deterred malicious cyber and EW activities and increased resilience of critical infrastructure
- Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts‡
- Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks‡
- Avoided alienation of population, military forces, and government in non-member states where NATO is operating‡
- Enhanced perceptions of NATO forces (in NATO countries and internationally)‡
- Increased partner cooperation‡
- Set standards for partner nations‡
- Reused captured infrastructure and materiel‡
- Avoided rebuilding costs‡
- Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent‡
- Enhanced NATO-wide public support for policies, objectives, and goals
- Achieved desired outcomes through influence on adversary militaries, governments, and populations
- Delayed, degraded, disrupted, manipulated, or precluded adversary actions
- Reduced effects of adversary attempts to delay, degrade, disrupt, manipulate, or preclude NATO and partner actions
- Projected power or demonstrated capabilities using IFCs
- Enhanced cyber, EW, IO, and NLW capabilities across all NATO members to deter, cooperate, deploy/sustain, and shape stability and peace

Strategic Goals

- Collectively deter and defend against aggression targeting member states
- Prevent and manage crises
- Achieve cooperative security

Color legend:

Primarily NLWs
Primarily IO
Primarily EW and cyber
Combined NLWs, IO, EW, and cyber

NOTE: ‡indicates that the element appeared in the previous NLW-centric logic model (see Romita Grocholski et al., 2022). ISR = intelligence, surveillance, and reconnaissance; C^{4}ISR = command, control, communications, computers, intelligence, surveillance, and reconnaissance.

- enhancing perceptions of U.S. forces, both domestically and internationally
- increasing cooperation with partners.

When we expanded the logic model to encompass the more expansive definition of IFCs for NATO, we found that many of the elements of the NLW logic model were also applicable to IO, EW, and cyber. This indicates that it makes sense to consider these technologies as a set of complementary capabilities, integrating them under the IFC umbrella.

The logic model also helps to support wargaming of IFCs, as was demonstrated in a NATO wargame. Overall, we found that there is a lot of potential value in wargaming IFCs, but there are a number of challenges that will need to be overcome in order to do this effectively. Success will require ensuring that players are familiar with the IFCs that are being used and have a clear understanding of the consequences of their uses, as well as any second-order effects. The information that would be provided to participants regarding IFC performance would stem from experiments, modeling, exercises, and real-world instances of IFC usage. Likewise, the contexts, scenarios, and levels of conflict of the wargame need to be crafted to elicit appropriate insights regarding the utility of these systems. We also found that integrating IFCs into M&S is likely best accomplished by developing new tools rather than attempting to fit them into existing tools that were designed with lethal weapons in mind. This is particularly true when considering the psychological effects of IFCs.

Recommendations

Our overarching recommendations are as follows:

- **Use the updated DoD-centric logic model, together with the vignettes and metrics described in the previous report, to help measure, document, and communicate the impact of NLWs within DoD.** The logic model provides a structure, now connected to the strategic goals of the 2022 NDS, to clarify how the activities that NLWs perform contribute to ultimate DoD aims. Measuring the values of metrics associated with those elements in real-world operations, exercises, and wargames can provide hard data with which to evaluate the impact of NLWs. The vignettes provide examples of NLW usage that can inform discussion throughout DoD, and also serve as a basis for wargames that further elucidate the impact of NLWs.
- **Use the NATO-centric logic model, metrics, and vignettes to help measure, document, and communicate the impact of IFCs within NATO.** All the points in the preceding bullet also apply in a NATO context, using the logic model, metrics, and vignettes that are tailored to NATO's needs. Those NATO-centric items both address NATO strategic goals and include all four types of IFCs (NLWs, IO, EW, and cyber).
- **Use aspects of the NATO-centric logic model, metrics, and vignettes to help shape DoD's development of the IFC concept.** DoD does not yet have a doctrinal definition of *intermediate force capabilities*. However, DoD personnel can use the NATO-centric materials that include NLWs, IO, EW, and cyber to help to think through how these types of capabilities interact with one another, contributing to development of an integrated, DoD-wide IFC concept. Only the NATO strategic goals need to be excised from consideration; the rest are still relevant to DoD.
- **Invest in M&S to support IFC wargames.** The accuracy of wargame results is predicated on having sufficient data regarding the effects of IFCs, from experiments, modeling, exercises, and/or real-world operations. Purpose-designed M&S that enable characterization of the psychological and other nonki-

netic effects of IFCs can provide valuable insights on its own, and can also contribute to adjudication of wargames involving IFCs.

- **Conduct wargames in which IFCs play an integrated role.** While NLWs have almost never been professionally wargamed, there is value in doing so. Integrating IFCs into wargames can provide insights on how IFCs could be used, their effectiveness in different contexts, the impact of using them in concert with other systems, and many other items. Game insights should be used to guide future lines of inquiry using other methodologies, rather than treated as final confirmation of IFC utility (or lack thereof). Wargames can also create awareness of IFCs among participants who might not previously have considered their utility. In conducting wargames that emphasize IFCs, we make three key recommendations:
  - Familiarize players with IFCs before the game and at its outset.
  - Ensure that the capabilities and effects of IFCs that are used in the game are supported by documentation, and that adjudication of their impact is credible.
  - Allow-for second-order effects of IFC usage (such as changed behavior to avoid exposure to IFCs) and direct adversary countermeasures to diminish IFCs' impact.

Contents

Figures and Tables

Figures

Tables

CHAPTER ONE

Introduction

Background

Non-lethal weapons (NLWs) comprise a highly diverse set of systems. Representative examples of NLWs are acoustic hailing devices, eye-safe laser dazzlers that create glare, flash-bang grenades, rubber bullets, millimeter-wave emitters that cause a temporary heating sensation, and entangling devices to stop vehicles or vessels. As was documented in a previous RAND report (Romita Grocholski et al., 2022), the U.S. Department of Defense (DoD) can employ NLWs for a range of purposes in a variety of contexts. That report also characterized how activities that employed NLWs ultimately contributed to DoD-wide strategic goals, using a structure called a *logic model*. The report also examined the potential usage of NLWs across a range of vignettes, as well as ways of measuring the impact of NLWs. The Joint Intermediate Force Capabilities Office (JIFCO), which sponsored this work and oversees NLW efforts for DoD, characterizes NLWs as part of a suite of *intermediate force capabilities* (IFCs), alongside electromagnetic warfare (EW), cyber, and information operations (IO).[1]

Purpose of This Study

JIFCO asked RAND to build on this prior work in three distinct respects. The first was to update the logic model so that it addressed the strategic goals enumerated in the 2022 National Defense Strategy (NDS), rather than the 2018 version of the NDS that had been used in the earlier version. The second was to create a new version of the logic model that would address the needs of the North Atlantic Treaty Organization (NATO). This would include all IFCs, including NLWs, EW, cyber, and IO, to better reflect the purview of the relevant NATO authorities. That logic model would also culminate in NATO strategic goals, rather than DoD ones. The third was to characterize how IFCs could be better integrated into wargames, as well as modeling and simulation (M&S). As part of this analysis, we would also support the development and documentation of IFC-centric wargames being run by NATO. This report describes the results of these three interrelated efforts.

Methodology

Each part of the analysis entailed a distinct methodology. To revise the DoD-centric logic model so that it would reflect the 2022 NDS, we first extracted the relevant strategic goals from a publicly available fact sheet on the new NDS (DoD, 2022; the full unclassified version of the NDS has not been made publicly available at

[1] Electromagnetic warfare is also a significant capability that is used in kinetic/lethal warfare. In the IFC context, we only refer to non-lethal use of this capability.

the time of writing in early 2022). We then linked these new strategic goals with other elements of the logic model.

The development of a NATO-centric IFC logic model required an expansion of the original logic model's scope to include IO, EW, and cyber defense. NATO focuses solely on cyber defense and resilience, therefore references to cyber in this report are to be considered only in the context of defense. We analyzed documents and interviewed subject-matter experts to identify elements of the logic model for these three additional warfare areas, then drew strategic goals from NATO documents. The new logic model, including the NLW-focused elements of the original version, was iteratively discussed with experts to validate and refine it. We developed 11 NATO-centric vignettes in order to confirm the utility of the logic model's elements in describing those vignettes; personnel supporting the NATO System Analysis and Studies Research Task Group (SAS-151) effort also used the vignettes to inform their analysis. The logic model was also used to support a NATO IFC wargame, which further corroborated its ability to describe the actions and effects taking place within the game. In addition, we analyzed which elements of the logic model related to one another, and to what degree, while also identifying several metrics for each element of the logic model.

Finally, we reviewed documents about wargaming and associated M&S, and also interviewed 26 experts, as a basis for analysis of integration of IFCs into these areas. The process of helping to develop and document the NATO IFC wargame also contributed to this analysis.

Structure of This Report

This report is structured around the three tasks mentioned above. Chapter Two describes the updated DoD-centric logic model, and Chapter Three covers the more extensively modified logic model for NATO purposes. Chapter Four addresses IFC integration into wargames and M&S. Chapter Five provides conclusions and recommendations. Following this, Appendix A provides an overview, as well as detailed tables, of the connections among elements of the NATO-centric logic model, and Appendix B provides a detailed description of the metrics that were identified to measure elements of that logic model. Appendix C describes the vignettes that were developed in tandem with the NATO IFC model. Appendix D provides a brief overview of non-lethal weapons. Finally, Appendix E describes two hypothetical game designs based on the vignettes listed in Appendix C.

CHAPTER TWO

Updated DoD Logic Model for Non-Lethal Weapons

In this chapter, we present the revised DoD-centric logic model, focusing exclusively on NLWs, but incorporating strategic goals from the 2022 NDS. We begin by explaining what a logic model is, how it is structured, and how it can be used. Next, we briefly explain how we updated the logic model from our previous study (Romita Grocholski et al., 2022), and present the new version, including how other elements of the logic model are linked to the new strategic goals. We then discuss how it differs from its predecessor, which used strategic goals based on the 2018 NDS.

Overview of a Logic Model

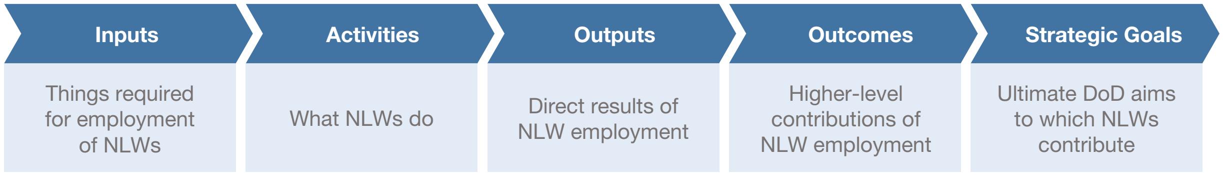
Logic models characterize how the activities of systems, processes, or organizations contribute to fulfillment of their goals. There are various types of logic models, but we are using a specific version based on a prior RAND publication, *Assessing Impact to Inform Decisions: A Toolkit on Measures for Policymakers* (Savitz, Matthews, and Weilant, 2017). In this type of logic model, a series of *inputs* enable *activities* that result in direct *outputs*, which contribute to higher-level *outcomes*, then to ultimate *strategic goals*. All these items are collectively termed *elements* of the logic model. Figure 2.1 shows how this applies in the context of NLWs.

This logic model was originally developed based on a review of over 150 documents on NLWs and interviews with 36 experts across range of organizations. We integrated findings from these sources in a series of internal workshops, and repeatedly refined them based on discussions with external experts and our own analyses. In general, logic models need to be modified over time to reflect evolving information about whatever they are describing, and the emergence of a new NDS is a perfect example of the need for such refinement.

As of early 2022, the 2022 NDS has not yet been made publicly available, though a fact sheet on it has (DoD, 2022). The fact sheet contains enough material to enable us to glean the strategic goals that we need for our purposes, even if it lacks some details. A classified version of the NDS is available, but we have deliberately chosen not to incorporate any information from it, so that our work can be presented in an unclassified report.

Table 2.1 compares the relevant strategic goals we derived from the 2018 and 2022 versions of the NDS. These are not ordered in terms of priority (which is unclear from publicly available documents), but based

FIGURE 2.1
Non-Lethal Weapon Logic Model Structure


Inputs
Things required for employment of NLWs
Activities
What NLWs do
Outputs
Direct results of NLW employment
Outcomes
Higher-level contributions of NLW employment
Strategic Goals
Ultimate DoD aims to which NLWs contribute

SOURCE: Savitz, Matthews, and Weilant, 2017.

TABLE 2.1

Strategic Goals Derived from the 2018 and 2022 National Defense Strategies

2018 NDS Strategic Goals	2022 NDS Strategic Goals
• Strengthen alliances and partnerships • Improve competitive advantage over adversaries • Seize the initiative to proactively expand the competitive space • Improve DoD's ability to compete below the level of armed conflict	• Strengthen alliances and partnerships • Improve competitive advantage over adversaries • Build a resilient joint force and defense ecosystem • Defend the homeland • Deter aggression and strategic attacks against the United States, allies, and partners • Prevail in conflict when necessary

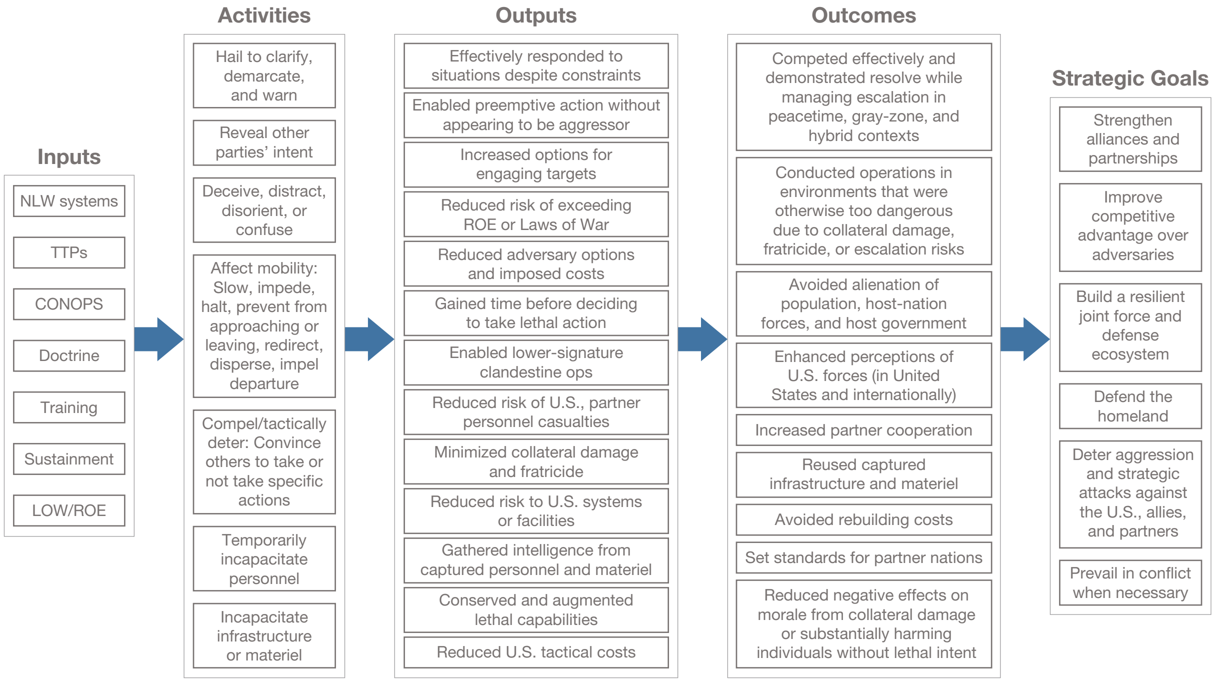
SOURCES: Mattis, 2018; DoD, 2022.

on similarity: The first two in each set are the same. Despite this commonality, the differences among the others are also evident. Given the sparse data that we have, it would be speculative to try to ascertain why the two sets of strategic goals differ as they do, and it would also be a diversion from our focus on NLWs. Rather, we incorporate these new strategic goals as they stand, without attempting to explain the reasoning behind them.

In Figure 2.2, we show the revised DoD-centric logic model, which includes the strategic goals from the 2022 NDS. The inputs listed in the leftmost column are the prerequisites for NLW usage, such as the systems themselves; training; doctrine; the tactics, techniques, and procedures (TTPs) and concepts of operations (CONOPS) that shape their usage; and other items. Given these inputs, personnel conduct a series of activi-

FIGURE 2.2

Revised DoD-Centric Logic Model with Strategic Goals from the 2022 National Defense Strategy


Inputs
NLW systems
TTPs
CONOPS
Doctrine
Training
Sustainment
LOW/ROE
Activities
Hail to clarify, demarcate, and warn
Reveal other parties' intent
Deceive, distract, disorient, or confuse
Affect mobility: Slow, impede, halt, prevent from approaching or leaving, redirect, disperse, impel departure
Compel/tactically deter: Convince others to take or not take specific actions
Temporarily incapacitate personnel
Incapacitate infrastructure or materiel
Outputs
Effectively responded to situations despite constraints
Enabled preemptive action without appearing to be aggressor
Increased options for engaging targets
Reduced risk of exceeding ROE or Laws of War
Reduced adversary options and imposed costs
Gained time before deciding to take lethal action
Enabled lower-signature clandestine ops
Reduced risk of U.S., partner personnel casualties
Minimized collateral damage and fratricide
Reduced risk to U.S. systems or facilities
Gathered intelligence from captured personnel and materiel
Conserved and augmented lethal capabilities
Reduced U.S. tactical costs
Outcomes
Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts
Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks
Avoided alienation of population, host-nation forces, and host government
Enhanced perceptions of U.S. forces (in United States and internationally)
Increased partner cooperation
Reused captured infrastructure and materiel
Avoided rebuilding costs
Set standards for partner nations
Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent
Strategic Goals
Strengthen alliances and partnerships
Improve competitive advantage over adversaries
Build a resilient joint force and defense ecosystem
Defend the homeland
Deter aggression and strategic attacks against the U.S., allies, and partners
Prevail in conflict when necessary

SOURCE: Adapted from Romita Grocholski et al., 2022.

NOTE: The right-most column is the only one that differs from the version of the logic model that was presented in the prior report. ROE = rules of engagement; LOW = Laws of War.

ties with NLWs, shown in the next column. For example, they use them to hail other parties, to distract them, to affect their mobility, or to temporarily incapacitate them. These result in the direct outputs shown in the third column. Outputs include the ability to respond effectively in constrained situations (such as when civilians and fighters are interspersed) or to create options and additional time for the U.S. side, while limiting the options of the other party. These outputs contribute to the higher-level outcomes in the fourth column, such as the ability to compete effectively in contexts short of war while managing the risk of escalating conflict with other powers, or enhanced perceptions of U.S. forces. Finally, those outcomes support the strategic goals of the DoD in the 2022 NDS, shown in the last column. As indicated, those are strengthening alliances and partnerships, improving DoD's competitive advantage, building a more resilient force, defending the homeland, deterring aggression and attacks, and prevailing when necessary. This last column is the only one that differs from the version of the logic model that was presented in the prior report.

Connections Among Elements of the Logic Model

In addition to identifying the elements of the logic model, we also delineated how those elements related to one another. Specifically, we noted the intensity with which elements in each column were linked to elements in adjacent columns. For that purpose, we used a three-point scale:

- 2: strong, unequivocal connection
- 1: limited, indirect, or conditional connection
- 0: no connection.

Our assessments of the intensity of these links were based on internal workshops, later validated by review by subject-matter experts. The results are shown in Figure 2.3, with thicker, darker lines indicating strong connections (2 on our scale) and thinner, lighter lines indicating more limited or indirect connections (1 on our scale). Our assessment was that *all* the inputs had strong connections to all the activities, so for reasons of clarity and space, we left the inputs out of the diagram. This is not meant to understate their importance; without essential inputs, such as sufficient training, none of these activities can occur.

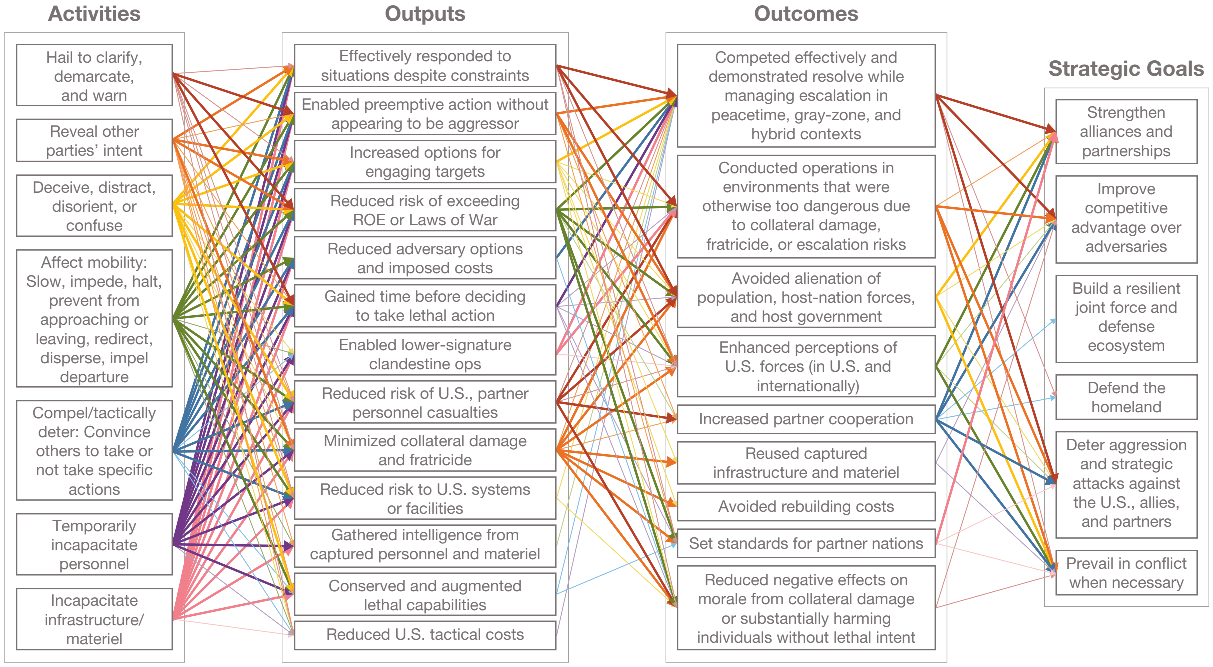
The activity-output and output-outcome connections are the same as were presented in the previous report, whereas the outcome-strategic goal links are new. Several patterns are clear. The first is that all seven activities provide strong support for multiple outputs, forming a dense thicket of lines, indicating that all of the activities are important. The links between outputs and outcomes are less dense, with the first nine outputs (out of 13) having strong links to the outcomes. The outcome-strategic goal links show that the first five outcomes (out of nine) are the ones that are most supportive of the strategic goals.

In Figure 2.4, we highlight the elements of the current logic model that have strong links to the next level—and thus, ultimately, to strategic goals—by encasing them in blue rectangles. All seven of the activities had strong connections to at least three outputs, while nine of the outputs had a strong connection to at least one outcome, and five of the outcomes had at least two strong connections to strategic goals. These 21 elements are the ones that should be most emphasized in assessing the impact of NLWs, as they can be used to make the strongest case for impacts at the strategic level. The density of links from those elements that ultimately lead to strategic goals demonstrates the degree to which they support those goals.

Figure 2.5 compares the outcome-strategic goal links for versions of the logic models using strategic goals from the 2022 and 2018 NDSs, also with the most relevant items encased in blue rectangles. The same five

FIGURE 2.3

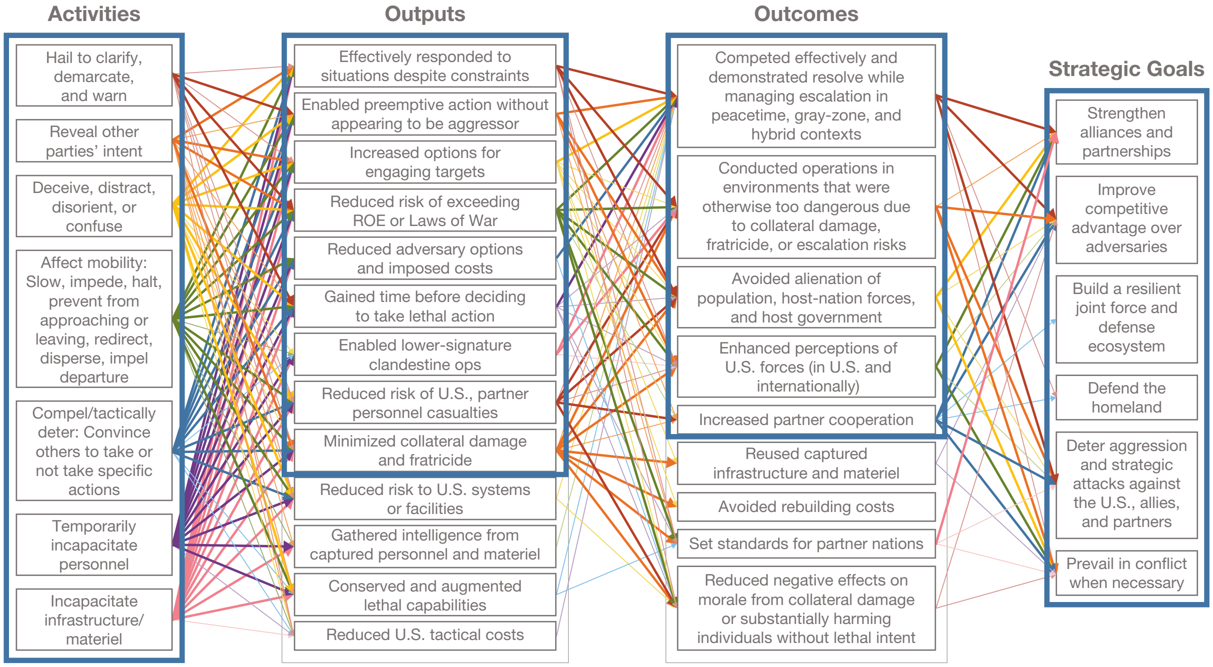
Connections Among the Levels of the DoD-Centric Logic Model


Activities
Hail to clarify, demarcate, and warn
Reveal other parties' intent
Deceive, distract, disorient, or confuse
Affect mobility: Slow, impede, halt, prevent from approaching or leaving, redirect, disperse, impel departure
Compel/tactically deter: Convince others to take or not take specific actions
Temporarily incapacitate personnel
Incapacitate infrastructure/ materiel
Outputs
Effectively responded to situations despite constraints
Enabled preemptive action without appearing to be aggressor
Increased options for engaging targets
Reduced risk of exceeding ROE or Laws of War
Reduced adversary options and imposed costs
Gained time before deciding to take lethal action
Enabled lower-signature clandestine ops
Reduced risk of U.S., partner personnel casualties
Minimized collateral damage and fratricide
Reduced risk to U.S. systems or facilities
Gathered intelligence from captured personnel and materiel
Conserved and augmented lethal capabilities
Reduced U.S. tactical costs
Outcomes
Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts
Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks
Avoided alienation of population, host-nation forces, and host government
Enhanced perceptions of U.S. forces (in U.S. and internationally)
Increased partner cooperation
Reused captured infrastructure and materiel
Avoided rebuilding costs
Set standards for partner nations
Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent
Strategic Goals
Strengthen alliances and partnerships
Improve competitive advantage over adversaries
Build a resilient joint force and defense ecosystem
Defend the homeland
Deter aggression and strategic attacks against the U.S., allies, and partners
Prevail in conflict when necessary

NOTE: Thick, dark lines indicate strong connections, and thinner, lighter lines indicate weaker ones. All lines emanating from a single element are shown in the same color, to facilitate visual tracking of their common source; the colors have no other meaning, and similar colors in different columns are unconnected.

FIGURE 2.4

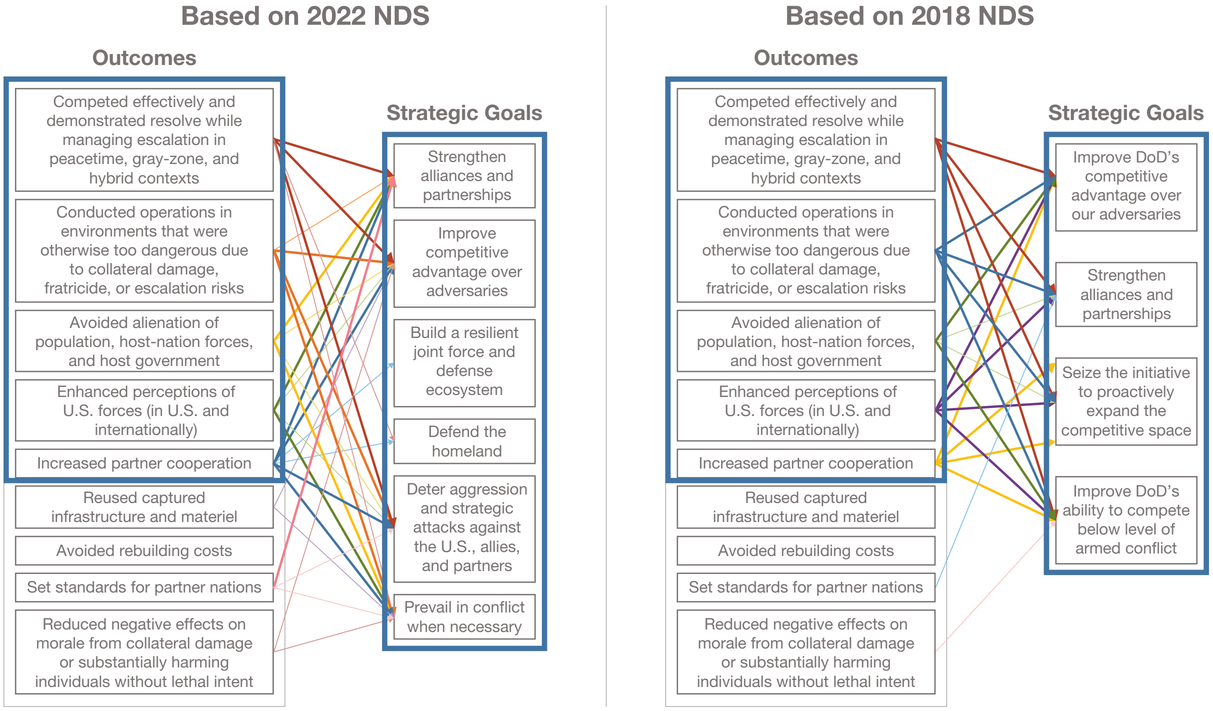
DoD-Centric Logic Model with Elements That Contribute Most to Strategic Goals Highlighted


Activities
Hail to clarify, demarcate, and warn
Reveal other parties' intent
Deceive, distract, disorient, or confuse
Affect mobility: Slow, impede, halt, prevent from approaching or leaving, redirect, disperse, impel departure
Compel/tactically deter: Convince others to take or not take specific actions
Temporarily incapacitate personnel
Incapacitate infrastructure/ materiel
Outputs
Effectively responded to situations despite constraints
Enabled preemptive action without appearing to be aggressor
Increased options for engaging targets
Reduced risk of exceeding ROE or Laws of War
Reduced adversary options and imposed costs
Gained time before deciding to take lethal action
Enabled lower-signature clandestine ops
Reduced risk of U.S., partner personnel casualties
Minimized collateral damage and fratricide
Reduced risk to U.S. systems or facilities
Gathered intelligence from captured personnel and materiel
Conserved and augmented lethal capabilities
Reduced U.S. tactical costs
Outcomes
Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts
Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks
Avoided alienation of population, host-nation forces, and host government
Enhanced perceptions of U.S. forces (in U.S. and internationally)
Increased partner cooperation
Reused captured infrastructure and materiel
Avoided rebuilding costs
Set standards for partner nations
Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent
Strategic Goals
Strengthen alliances and partnerships
Improve competitive advantage over adversaries
Build a resilient joint force and defense ecosystem
Defend the homeland
Deter aggression and strategic attacks against the U.S., allies, and partners
Prevail in conflict when necessary

NOTE: Thick, dark lines indicate strong connections, and thinner, lighter lines indicate weaker ones. All lines emanating from a single element are shown in the same color, to facilitate visual tracking of their common source; the colors have no other meaning, and similar colors in different columns are unconnected.

FIGURE 2.5

Comparison of Links Between Outcomes and Strategic Goals, with Strategic Goals from Both the 2022 and 2018 Versions of the National Defense Strategy


Based on 2022 NDS
Outcomes
Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts
Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks
Avoided alienation of population, host-nation forces, and host government
Enhanced perceptions of U.S. forces (in U.S. and internationally)
Increased partner cooperation
Reused captured infrastructure and materiel
Avoided rebuilding costs
Set standards for partner nations
Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent
Strategic Goals
Strengthen alliances and partnerships
Improve competitive advantage over adversaries
Build a resilient joint force and defense ecosystem
Defend the homeland
Deter aggression and strategic attacks against the U.S., allies, and partners
Prevail in conflict when necessary
Based on 2018 NDS
Outcomes
Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts
Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks
Avoided alienation of population, host-nation forces, and host government
Enhanced perceptions of U.S. forces (in U.S. and internationally)
Increased partner cooperation
Reused captured infrastructure and materiel
Avoided rebuilding costs
Set standards for partner nations
Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent
Strategic Goals
Improve DoD's competitive advantage over our adversaries
Strengthen alliances and partnerships
Seize the initiative to proactively expand the competitive space
Improve DoD's ability to compete below level of armed conflict

NOTE: Thick, dark lines indicate strong connections, and thinner, lighter lines indicate weaker ones. All lines emanating from a single element are shown in the same color, to facilitate visual tracking of their common source; the colors have no other meaning, and similar colors in different columns are unconnected.

outcomes were most supportive of the strategic goals for the 2018 and 2022 versions of the NDS. This stability is reassuring: It suggests that these outcomes' importance is enduring, even as departmental aims evolve.[1]

In the prior report (Romita Grocholski et al., 2022), we identified 97 metrics that collectively measured the activities, outputs, and outcomes of the logic model. These metrics remain useful for that purpose and do not require updates based on the revision of the logic model's strategic goals. Identifying metrics for DoD-wide strategic goals is beyond our scope: Those should be selected at the highest levels of DoD. We also had not identified input metrics, which were either existing technical specifications or irrelevant for evaluating NLWs' impact. The vignettes that we had developed for exploration of the DoD logic model, and for evaluation of the metrics, also remain unchanged and can be found in the previous report.

[1] One of the outcomes that had lacked a strong connection to any of the 2018 strategic goals had a strong connection to one of the 2022 ones: Specifically, "Set standards for partner nations" had a strong connection to "Strengthen alliances and partnerships." This could potentially have elevated it to inclusion in the blue box. However, because all of the other outcomes in question had at least two strong connections to strategic goals, we continued to group this borderline case with outcomes that lacked strong connections altogether, recognizing that others might group it differently.

CHAPTER THREE

NATO Logic Model, Metrics, and Vignettes for IFCs

JIFCO asked RAND to develop a NATO-specific model in support of a NATO System Analysis and Studies Research Task Group (SAS-151), whose formal title is "Solutions Enabling Intermediate Force/Non-Lethal Weapon Contributions to Mission Success." SAS-151 conducted various analytical activities, including wargames, to support development of a NATO Intermediate Force Capability Concept. It worked closely with JIFCO and many other national establishments, and was sponsored by the NATO Collaboration Support Office.

There are two key differences between the NATO-centric and DoD-centric versions of these materials. The first stems from NATO's definition of IFCs: "Active means below lethal intent that temporarily impair, disrupt, delay, or neutralize targets across all domains and all phases of competition and conflict" (NATO, 2022a). This definition encompasses EW, cyber, and IO, as well as NLWs, so the NATO version of the logic model includes all of these warfare areas, whereas the DoD version only includes NLWs. The second difference is that, naturally, the logic model's strategic goals need to be derived from NATO documents, rather than from DoD sources.

In this chapter, we first present the NATO-centric IFC logic model, then discuss the associated vignettes and metrics. The connections between logic model elements are discussed further in Appendix A, the metrics are further discussed in Appendix B, while more details on the vignettes appear in Appendix C.

NATO-Centric Logic Model

Development of the Logic Model

There were several steps in developing the NATO-centric IFC logic model. Multiple individuals involved in NATO's SAS-151 effort reviewed the DoD-centric NLW logic model, confirming that, except for the strategic goals, it aligned with NATO's existing concepts regarding NLWs; this was corroborated by our review of SAS-151's draft IFC concept. The original logic model was therefore expanded upon, with only slight changes in wording—for example, references to NATO supplanting those to U.S. forces. Various documents and interviews about IO, EW, and cyber helped us to identify additional elements of the logic model to address those warfare areas, which we cite in the following pages and in the references section of the report. NATO documents also provided strategic goals that were incorporated into the logic model (NATO, Public Diplomacy Division, 2010; NATO, 2020). The entire logic model was then shared with NATO and other experts to garner feedback that enabled its refinement. A final corroboration took place during an SAS-151 wargame in November 2021, when 45 of the logic model's 60 activities, outputs, and outcomes were observed during the course of the game. Fully 23 of those were observed on at least ten separate occasions.

Structure of the Logic Model

Below, we present the structure of the logic model. For those who may only be reading this chapter, a brief overview of logic models in general and their structure appears toward the beginning of Chapter Two and may be worth quickly perusing. To summarize it in a single sentence (reiterating the point for those who have read Chapter Two), the logic model links *inputs* that enable *activities*, whose direct *outputs* contribute to higher-level *outcomes* and ultimate *strategic goals*.

Throughout our presentation of the logic model, we use the following color scheme and symbology:[1]

- Elements that primarily relate to NLWs are shown in purple.
- Elements that primarily relate to IO are shown in orange.
- Elements that primarily relate to EW and cyber are shown in teal.
- Elements that relate to NLWs, IO, EW, and cyber are shown in green.
- Elements that appeared in the DoD-centric model are marked with a double dagger.‡

We have grouped EW and cyber together in this color scheme after ascertaining that within the logic model, the elements that related to one often related to the other. We do not provide color coding for the other potential groupings (e.g., elements that primarily relate to NLWs and IO, but not the other two) because there were no logic model elements that could be categorized in those groupings.

Inputs

The inputs—items that are prerequisites for IFC usage—are listed below:

- Elements that relate to NLWs, IO, EW, and cyber
  - IFC systems‡
  - Concepts of operations (CONOPS) and employment (CONEMP)‡
  - Tactics, techniques, and procedures (TTPs)‡
  - Doctrine‡
  - Training‡
  - Sustainment‡
  - Domain-specific expertise
  - Industrial base
  - Intelligence, surveillance, and reconnaissance (ISR)
  - Integration into warfighting processes
- Elements that primarily relate to IO
  - Communications platforms and media
- Elements that primarily relate to EW and cyber
  - Network infrastructure and software.

All the inputs from the DoD logic model that focused on NLWs were not only retained in the NATO logic model, but turned out to be applicable to not just NLWs but to IO, EW, and cyber as well, which is why there are no NLW-specific (purple) items listed in the inputs. Many of the inputs that were added to the NATO logic model are relevant for all types of actions, but we decided to include them in the logic model to reflect their importance to IO, EW, and cyber. EW and cyber require individuals with tremendous depth of specific expertise, plus a modicum of training for other personnel, as well as an industrial base that can provide very precise, noncommercial equipment for EW. Intelligence, surveillance, and reconnaissance (ISR) is a particularly critical need for EW and cyber, given the need to understand adversary networks and their threats to

[1] We use color-coding in the figures because of space allowances. In the bulleted lists in this chapter and in Chapter Four, we also repeat the meanings of the colors, for the benefit of readers with color vision deficiency.

NATO's own. The ability to communicate with the public is critical for IO, while EW and cyber require network infrastructure and appropriate software.

Activities

The activities that are performed using IFCs are listed below:

- Elements that primarily relate to NLWs
  - Hail to clarify, demarcate, and warn‡
  - Reveal other parties' intent‡
  - Affect mobility: Slow, impede, halt, prevent from approaching or leaving, redirect, disperse, impel departure‡
  - Compel/tactically deter: Convince others to take or not take specific actions‡
  - Temporarily incapacitate personnel‡
  - Incapacitate infrastructure/materiel‡
- Elements that primarily relate to IO
  - Disseminate information to inform and persuade
  - Disseminate information to affect adversary perceptions and assessments
  - Expose malign information operations
- Elements that primarily relate to EW and cyber
  - Detect and identify sources of electromagnetic (EM) radiation
  - Characterize, locate, and track sources of EM radiation
  - Conduct reconnaissance against, exploit, and establish persistent presence in adversary systems to prepare the cyber battlespace
  - Defend/protect/remediate NATO front-line systems against EW
  - Defend and remediate NATO networks and critical infrastructure (e.g., data backbone) against cyber and EW (includes diagnosis of issues)
  - Secure, configure, maintain, and protect existing networks to prevent attacks
- Elements that relate to NLWs, IO, EW, and cyber
  - Deceive, distract, disorient, or confuse‡
  - Degrade, disrupt, and destroy adversary systems and C^4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance).

The first few activities, in purple, are taken from the prior logic model on NLWs. The next three, in orange, relate to inherent parts of the IO mission, namely disseminating information and countering disinformation. The activities in teal involve gaining information about adversary actions and networks while protecting NATO's. The last two items, in green, relate to disruption of the adversary, and apply to all four warfare areas. The next-to-last is taken from the prior logic model, but the deception and disorientation that it entails turns out to be broadly applicable, as is targeting adversary systems and C^4ISR.

Outputs

The direct outputs resulting from the above activities appear below:

- Elements that relate to NLWs, IO, EW, and cyber
  - Effectively responded to situations despite constraints‡
  - Enabled pre-emptive action without appearing to be aggressor‡
  - Increased options for engaging targets‡
  - Reduced risk of exceeding ROE or Laws of War‡

  - Reduced adversary options and imposed costs‡
  - Gained time/distance before deciding to take lethal action‡
  - Enabled lower-signature clandestine ops‡
  - Reduced risk of NATO, partner personnel casualties‡
  - Minimized collateral damage and fratricide‡
  - Reduced risk to NATO systems or facilities‡
  - Gathered intelligence from captured personnel and materiel, as well as from cyber and EW means‡
  - Conserved and augmented lethal capabilities‡
  - Reduced NATO tactical costs (broadly defined)‡
  - Disrupted adversary decision cycle to provide relative advantage to NATO forces and degrade adversary ability to employ forces effectively‡
- Elements that primarily relate to IO
  - Affected perceptions, decisionmaking, and behavior of adversary leadership
  - Affected perceptions, decisionmaking, and behavior of adversary personnel
  - Affected adversary leadership's emotional state, judgement, and will to fight
  - Affected adversary personnel's emotional state, judgement, and will to fight
  - Avoided effects of adversary manipulation of information to affect perceptions, attitudes, decisions, and behaviors of NATO and partner forces
  - Avoided effects of adversary manipulation of information to affect perceptions, decisionmaking, and behavior of populations in NATO members, partner nations, and neutral nations
  - Influenced perceptions, decisionmaking, and behavior of populations
- Elements that primarily relate to EW and cyber
  - Achieved knowledge of adversary networks
  - Created actionable objectives in adversary networks to facilitate their potential disruption/degradation/destruction (potentially prior to conflict)
  - Disrupted, degraded, manipulated, and/or destroyed adversary networks
  - Minimized disruption, degradation, manipulation, and destruction of networks and systems, as well as recovery time and costs, from EW and/or cyberattack.

The outputs that had been originally developed for NLWs alone in the original DoD logic model (indicated by a double dagger) turned out to have been versatile, applying to all four categories of IFCs, which is why they are green in the list above. For example, all four types of IFCs can increase options while constraining those of the adversary. The IO-specific outputs, in orange, related to having influenced others and having countered adversary influence efforts. The outputs addressing EW and cyber, in teal, addressed the degree to which adversary networks had been penetrated or affected, as well as the degree of avoidance of the same for NATO networks.

Outcomes

The higher-level outcomes to which the above outputs achieve are listed below:

- Elements that relate to NLWs, IO, EW, and cyber
  - Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts‡
  - Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks‡
  - Avoided alienation of population, military forces, and government in non-member states where NATO is operating‡

  - Enhanced perceptions of NATO forces (in NATO countries and internationally)‡
  - Increased partner cooperation‡
  - Set standards for partner nations‡
  - Reused captured infrastructure and materiel‡
  - Avoided rebuilding costs‡
  - Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent‡
  - Enhanced NATO-wide public support for policies, objectives, and goals
  - Achieved desired outcomes through influence on adversary militaries, governments, and populations
  - Delayed, degraded, disrupted, manipulated, or precluded adversary actions
  - Reduced effects of adversary attempts to delay, degrade, disrupt, manipulate, or preclude NATO and partner actions
  - Projected power or demonstrated capabilities using IFCs
  - Enhanced cyber, EW, IO, and NLW capabilities across all NATO members to deter, cooperate, deploy/sustain, and shape stability and peace
- Elements that primarily relate to IO
  - Maintained credibility and legitimacy of NATO and partner forces
  - Reduced credibility and legitimacy of adversaries
- Elements that primarily relate to EW and cyber
  - Prevented and deterred malicious cyber and EW activities and increased resilience of critical infrastructure.

Outcomes turned out to be highly versatile: 15 out of the 18 of them applied across all four categories of IFCs, including all of the outcomes that had originally been designed for NLWs alone. This stems from a common feature of IFCs, namely that, compared with many kinetic weapons, they generally achieve their impact while limiting the amount of permanent damage to humans, and often to buildings or systems. A couple of outcomes related primarily to IO, and one related primarily to EW and cyber.

Strategic Goals

From the *NATO 2022 Strategic Concept* (NATO, 2022b), we identified three NATO-wide strategic goals, which the *Strategic Concept* describes as the alliance's "core tasks":

- Collectively deter and defend against aggression targeting member states.
- Prevent and manage crises.
- Achieve cooperative security.

Although these are distinct from DoD strategic goals, there is also a lot in common. NATO's goal of deterring and defending against aggression is essentially the same as one of DoD's goals, and NATO's aim of achieving collective security aligns closely with DoD's goal of strengthening alliances and partnerships.

Overview of the Entire Logic Model

Figure 3.1 shows the NATO-centric IFC logic model as a whole, encompassing all the items listed above. It is far more voluminous than the DoD-centric, NLW-specific logic model presented in Chapter Two, with 75 elements, compared to the earlier logic model's 42.

FIGURE 3.1
All Elements of the NATO-Centric Logic Model

Inputs

- Communications platforms and media
- Network infrastructure and software
- Integration into warfighting processes
- Domain-specific expertise
- Industrial base
- IFC systems‡
- Concepts of operations (CONOPS) and employment (CONEMP)‡
- Tactics, techniques, and procedures‡
- Doctrine‡
- Training‡
- Sustainment‡
- ISR‡

Activities

- Hail to clarify, demarcate, and warn‡
- Reveal other parties' intent‡
- Affect mobility: Slow, impede, halt, prevent from approaching or leaving, redirect, disperse, impel departure‡
- Compel/tactically deter: Convince others to take or not take specific actions‡
- Temporarily incapacitate personnel‡
- Incapacitate infrastructure/materiel‡
- Disseminate information to inform and persuade
- Expose malign information operations
- Disseminate information to affect adversary perceptions and assessments
- Detect and identify sources of electromagnetic (EM) radiation
- Characterize, locate, and track sources of EM radiation
- Conduct reconnaissance against, exploit, and establish persistent presence in adversary systems to prepare the cyber battlespace
- Defend/protect/remediate NATO front-line systems against EW
- Defend and remediate NATO networks and critical infrastructure (e.g., data backbone) against cyber and EW (includes diagnosis of issues)
- Secure, configure, maintain, and protect existing networks to prevent attacks
- Deceive, distract, disorient, or confuse‡
- Degrade, disrupt, and destroy adversary systems and C^4ISR

Outputs

- Affected perceptions, decisionmaking, and behavior of adversary leadership
- Affected perceptions, decisionmaking, and behavior of adversary personnel
- Affected adversary leadership's emotional state, judgement, and will to fight
- Affected adversary personnel's emotional state, judgement, and will to fight
- Avoided effects of adversary manipulation of information to affect perceptions, attitudes, decisions, and behaviors of NATO and partner forces
- Avoided effects of adversary manipulation of information to affect perceptions, decisionmaking, and behavior of populations in NATO members, partner nations, and neutral nations
- Influenced perceptions, decisionmaking, and behavior of populations
- Achieved knowledge of adversary networks
- Created actionable objectives in adversary networks to facilitate their potential disruption/degradation/destruction (potentially prior to conflict)
- Disrupted, degraded, manipulated, and/or destroyed adversary networks
- Minimized disruption, degradation, manipulation, and destruction of networks and systems, as well as recovery time and costs, from EW and/or cyberattack
- Effectively responded to situations despite constraints‡
- Enabled pre-emptive action without appearing to be aggressor‡
- Increased options for engaging targets‡
- Reduced risk of exceeding rules of engagement or Laws of War‡
- Reduced adversary options and imposed costs‡
- Gained time/distance before deciding to take lethal action‡
- Enabled lower-signature clandestine ops‡
- Reduced risk of NATO, partner personnel casualties‡
- Minimized collateral damage and fratricide‡
- Reduced risk to NATO systems or facilities‡
- Gathered intelligence from captured personnel and materiel, as well as from cyber and EW means‡
- Conserved and augmented lethal capabilities‡
- Reduced NATO tactical costs (broadly defined)‡
- Disrupted adversary decision cycle to provide relative advantage to NATO forces and degrade adversary ability to employ forces effectively

Outcomes

- Maintained credibility and legitimacy of NATO and partner forces
- Reduced credibility and legitimacy of adversaries
- Prevented and deterred malicious cyber and EW activities and increased resilience of critical infrastructure
- Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts‡
- Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks‡
- Avoided alienation of population, military forces, and government in non-member states where NATO is operating‡
- Enhanced perceptions of NATO forces (in NATO countries and internationally)‡
- Increased partner cooperation‡
- Set standards for partner nations‡
- Reused captured infrastructure and materiel‡
- Avoided rebuilding costs‡
- Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent‡
- Enhanced NATO-wide public support for policies, objectives, and goals
- Achieved desired outcomes through influence on adversary militaries, governments, and populations
- Delayed, degraded, disrupted, manipulated, or precluded adversary actions
- Reduced effects of adversary attempts to delay, degrade, disrupt, manipulate, or preclude NATO and partner actions
- Projected power or demonstrated capabilities using IFCs
- Enhanced cyber, EW, IO, and NLW capabilities across all NATO members to deter, cooperate, deploy/sustain, and shape stability and peace

Strategic Goals

- Collectively deter and defend against aggression targeting member states
- Prevent and manage crises
- Achieve cooperative security

Color legend:

Primarily NLWs
Primarily IO
Primarily EW and cyber
Combined NLWs, IO, EW, and cyber

NOTE: ‡indicates that the element appeared in the previous NLW-centric logic model (see Romita Grocholski et al., 2022).

Connections Among Levels of the Logic Model

As with the DoD-centric, NLW-focused logic model, we used a three-point scale to characterize the degree to which each element of the logic model was linked to elements in adjacent levels:

- 2: strong, direct, unequivocal connection
- 1: limited, indirect, or conditional connection
- 0: no connection.

We conducted a series of internal workshops to evaluate the intensity of these connections, then shared our findings with NATO and JIFCO subject-matter experts for validation.

The map of connections among the various levels of the logic model is complex, with 75 elements joined by 646 connections, so we present it in stages in Appendix A to make each portion of it accessible. The most important point that emerged from this is that we were able to see which elements of the logic model had a plethora of strong connections that ultimately linked them to the strategic goals. Given the large number of logic model elements with at least one chain of strong connections linking them to strategic goals (51 out of 75), we decided we needed to update our methodology for identifying key logic model elements. Rather than focusing on which elements had any strong connections to the next level, as was described in the previous chapter, we raised the threshold for the number of strong connections required to indicate an element that was well-linked. To determine which elements should be considered to be key elements, we selected thresholds for the minimum number of strong connections that would differentiate roughly one-third of the elements in any given level from the others (6 of 17 activities, 8 of 25 outputs, and 7 of the 18 outcomes). We list the elements that met these thresholds in Table 3.1.

These 21 elements, out of a total of 60 activities, outputs, and outcomes, are the ones that are best linked to NATO's strategic goals. When personnel supporting NATO want to evaluate the impact of IFCs, or to discuss their impact, these are the elements they should emphasize.

Measuring Elements of the Logic Model

We have expanded the number of metrics that can be used to evaluate IFCs in a NATO context, including metrics for the elements relating to EW, cyber, and IO. Each of these metrics, as well as the NLW-related metrics, are listed, along with their corresponding activity, output, or outcome, in Appendix B. We discuss the overall characteristics of the new metrics here.

Overall, we identified 153 new metrics that can be used to measure the 31 new activities, outputs, and outcomes in the NATO logic model. The breakdown of these numbers by type of element is shown in Table 3.2. We also identified seven metrics originally designed to measure elements from the previous logic model that were applicable to the more expansive definition of IFCs in order to ensure that there were metrics that measured all aspects of these capabilities.

Generally, we found that the metrics for activities relating to EW and cyber focused on measuring the detection and characterization of systems, as well as whether those systems were affected by the adversary, while metrics for activities relating to IO were focused on measuring the receipt and interpretation of information. At the output level, the metrics for EW and cyber were largely focused on measuring the extent and nature of impacts (e.g., duration, disruption, destruction), and metrics for IO focused on measuring the behavior of target populations. Finally, the metrics relating to EW- and cyber-related outcomes largely measured how NATO and adversary actions and options are affected by damage to their systems, and the metrics relating to IO-related outcomes focused on measuring perceptions of targeted populations, as measured by polls and online activity. Table 3.3 provides examples of these kinds of metrics for three new logic model

TABLE 3.1
Elements with the Highest Numbers of Strong Connections to Strategic Goals

Activities with at Least 10 Strong Connections to Outputs	Outputs with at Least 5 Strong Connections to Outcomes	Outcomes Connected to All 3 Strategic Goals, with Strong Connections to at Least 2
• Affect mobility • Compel/tactically deter • Temporarily incapacitate personnel • Incapacitate infrastructure/materiel • Deceive, distract, disorient, or confuse • Degrade, disrupt, and destroy adversary systems and C^4ISR	• Effectively responded to situations despite constraints • Enabled pre-emptive action without appearing to be aggressor • Reduced risk of exceeding ROE or Laws of War • Minimized collateral damage and fratricide • Disrupted adversary decision cycle to provide relative advantage to NATO forces and degrade adversary ability to employ forces effectively • Avoided effects of adversary manipulation of information to affect NATO and partner forces • Avoided effects of adversary manipulation of information to affect populations • Influenced perceptions, decisionmaking, and behavior of populations	• Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts • Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks • Maintained credibility and legitimacy of NATO and partner forces • Reduced effects of adversary attempts to delay, degrade, disrupt, manipulate, or preclude NATO and partner actions • Projected power or demonstrated capabilities using IFCs • Prevented and deterred malicious cyber and EW activities and increased resilience of critical infrastructure • Enhanced cyber, EW, IO, and NLW capabilities across all NATO members to deter, cooperate, deploy/sustain, and shape stability and peace

TABLE 3.2
Number of New Elements and Metrics by Logic Model Element Type

Type of Element	Number of New Elements	Number of New Metrics
Activities	10	66
Outputs	12	48
Outcomes	9	39

elements (one activity, one output, and one outcome). Different metrics require very different ways of assessing their values. For example, a cyber team with access to an adversary system may be able to detect when that system has been degraded by its actions and to what extent it has been degraded, using highly classified technical means. On the other hand, characterizing public sentiment can be done through open polling or unclassified observation of social media trends.

We used the same criteria as the previous study to evaluate metrics on a three-point scale (high, medium, low) in terms of their validity, reliability, feasibility, and timeliness. The criteria for these assessments are summarized in Table 3.4.

We found that nearly all the metrics were good measures of their associated logic model elements, with 85 percent of the metrics rating high in terms of their validity. In terms of feasibility and timeliness, the quality of the metrics depended on the IFC that they were attempting to measure. Cyber metrics are comparatively quick and easy to measure. EW metrics are harder to measure because of uncertainty regarding how quickly and accurately electromagnetic emissions can be characterized. IO metrics are generally quite

TABLE 3.3

Examples of Metrics Associated with a Subset of Elements of the NATO Logic Model

Type of Element	Element Description	Metric
Activity	Degrade, disrupt, and destroy adversary systems and C^{4}ISR	Number of non-targeted systems affected
		Timeline between IFC use and impact
		Percentage of targeted adversary systems and C^{4}ISR degraded, and/or disrupted
		Percentage of targeted adversary systems and C^{4}ISR destroyed
		Percentage of targeted adversary systems and C^{4}ISR exploited
		Percentage of attempts to degrade, disrupt, destroy, or exploit adversary systems and C^{4}ISR that the adversary successfully prevents or mitigates
Output	Influenced perceptions, decisionmaking, and behavior of populations	Percentage of population perceiving content of IO campaign as accurate (measured by polls)
		Percentage of population agreeing with content of IO campaign and considering it important (measured by polls)
		Number of people resharing content from IO campaign via social media
		Percentage of populations indicating negative perceptions of adversary in ways that reflect IO campaign (measured by polls)
		Number and scale of protests against adversary actions in adversary nation(s)
		Number of media articles reflecting content of IO campaign
		Number of lawsuits against individuals or governments that reflect content of IO campaign
		Number of political mobilization efforts reflecting agreement with content of IO campaign
Outcome	Enhanced NATO-wide public support for policies, objectives, and goals	Percentages of NATO member states' populations supporting NATO policies, objectives, and goals, as measured by polls
		Variation in percentage of NATO member population that supports NATO policies, objectives, and goals across NATO members, as measured by polls
		Number of public incidents (e.g., protests) within NATO states that indicate opposition to NATO policies, objectives, or goals
		Percentage of population in NATO member states that supports maintaining or increasing levels of funding
		Percentage of population in NATO member states that supports NATO membership

difficult and time-consuming to measure because they often involve assessing how human beings relate to and engage with information.

TABLE 3.4

Criteria for Evaluating Validity, Reliability, Feasibility, and Timeliness of Metrics

	Validity	Reliability	Feasibility	Timeliness[a]
High	Directly measures the element or a close proxy	Well-defined, objective, and stable	Required data sets are readily available and user-friendly	Hours
Medium	Closely related to the element being measured	Some ambiguity, subjectivity, and/or volatility	Required data sets could be collected with limited effort	Days
Low	Indirectly related to the element being measured	Considerable ambiguity, subjectivity, and/or volatility	Required data sets would be challenging to collect	Weeks to years

SOURCE: Savitz, Matthews, and Weilant, 2017.

[a] This refers to the timeliness of receipt of the values of metrics, not timeliness of the effects of IFCs. We selected the values for high, medium, and low timeliness as follows. Values of metrics that are received within hours can inform short-term tactical decisions. Those that are available within days may affect larger operational activities. Those that take weeks or longer can inform future operations.

NATO-Centric Vignettes

We developed a series of 11 vignettes associated with the logic model, for three purposes. First, having a set of concrete vignettes helped us to validate the logic model, by enabling us to think through whether the elements of the logic model would encompass all aspects of the vignettes. Second, these vignettes were intended to be useful in illustrating contexts of IFC usage in a NATO context, and we received positive feedback from personnel involved in SAS-151 regarding the vignettes' value. Third, these can be helpful to wider audiences in considering how IFCs can be used to address these diverse situations. They can be used to stimulate discussions: for example, to explore how to shape IFC CONOPS, TTPs, or acquisition in order to be able to better address particular situations. They can also serve as a basis for wargames, either by expanding a single vignette or concatenating several of them.

The 11 vignettes are listed in Table 3.5, together with a brief description for each. Detailed descriptions of each of vignette appear in Appendix C. By design, these vignettes collectively entail use of NLWs, IO, EW, and cyber capabilities, and most involve multiple capabilities. They reflect a range of missions, challenges, operational contexts, and geographic regions in which NATO may employ these capabilities. While none employ the real names of specific countries, most of those with somewhat identifiable locations take place either in Europe or areas that are relatively close to that continent, reflecting many of NATO's emphases.

There are a couple of overarching points that emerged from our development and review of these vignettes. First, IFCs were relevant in a wide range of potential NATO contexts in the vignettes we created, even in non-intuitive ones—for example, NLWs were used during full-scale combat in "Not Quiet on the Eastern Front." Second, we found that many of the potential uses of different types of IFCs were complementary and even synergistic. For example, in "Gently Seizing Control of the Very Dangerous Weapons," cyber and EW contributed to incapacitation of key adversary systems, facilitating the use of NLWs to take control of a facility without explosives or guns that might release chemical or biological agents. This overall approach also contributed to an IO campaign that would maximize positive perceptions of NATO. Overall, then, we identified diverse situations in which IFCs could benefit NATO, and our analysis indicated that the conception of NLWs, IO, EW, and cyber as belonging under a single IFC umbrella had value, insofar as they can contribute to each other's success.

TABLE 3.5

Vignettes for the NATO-Centric Logic Model

Vignette	Description
Don’t Beam Me Up	In a small nation that hosts bases from many other powers, forces from one of those powers are targeting NATO forces using microwave beams, aiming blinding lasers at aircraft and ships, and using EW to crash uncrewed aerial vehicles (UAVs).
Order on the Border	NATO forces on the border between a NATO member and hostile nation are trying to get migrants not to cross in unauthorized locations.
Hazy Shade of Winter	A ransomware cyberattack has shut down NATO nations’ facilities for handling liquefied natural gas imports.
Gently Seizing Control of the Very Dangerous Weapons	NATO forces are attempting to use multiple IFCs to seize a facility for manufacturing and storing chemical and biological weapons, while trying to minimize the risk of releases and aiming to capture systems, personnel, and computer systems intact.
Tanks, but No Tanks	NATO forces are using various IFCs to impede the advance of tanks from a hostile nation into a partner nation.
A Friend in Need or a Foe Indeed	Boats departing from a war-torn nation are approaching a NATO warship, but it is unclear whether the boat contains migrants or potential terrorists who may want to launch a suicide attack.
Perplexing Perimeter Protection Problems	Deployed NATO forces are considering use of various IFCs to deter locals from stealing fencing and security equipment from base perimeters.
Northern Exposure	NATO forces are trying to help a NATO member restore order in an Arctic territory over which it has sovereignty, despite protests instigated by a hostile nation.
Balkan Blues	NATO forces are using multiple IFCs to try to prevent fighting between two groups in the Balkans.
Nightmare at the Museum	NATO forces are trying to counter an attempt by personnel in unmarked uniforms from Vermilion to infiltrate and take over NATO member Fractus.
Not Quiet on the Eastern Front	A nation adjoining several NATO members has launched a full-scale invasion of their territories, and Article V has been invoked. In the heat of large-scale combat, NATO forces are using IFCs to complement more traditional weapons.

CHAPTER FOUR

IFCs and Wargaming

In this chapter, we discuss how wargaming could be incorporated into IFC research and adoption within DoD. There are many definitions for *wargaming*, varying in emphasis and scope; one found in the influential wargaming text by Peter Perla, *The Art of Wargaming*, reads,

> a wargame is a warfare model or simulation whose operation does not involve the activities of actual military forces, and whose sequence of events affects and is, in turn, affected by the decisions made by players representing the opposing sides. (Perla, 1990)

While modern wargames are not always confined to studying the interaction of two adversaries in a conflict, the competitive interplay between teams within the context of a specific scenario is a key characteristic of wargames that provides unique opportunities for studying human decisionmaking and perceptions, as well as an engaging educational environment.

To identify how IFCs might be integrated into DoD wargames, we interviewed 26 wargamers with a wide range of expertise. A synthesis of their insights is presented here, covering when and why it makes sense to include IFCs in games, the current state of IFC-related wargaming within DoD, and how IFCs could be successfully integrated into future DoD wargames. Two hypothetical games are described in Appendix E to further stimulate thought on integrating IFCs into wargaming. Our conversations with wargaming experts also informed a brief discussion of IFC-related M&S, both in support of wargames and as standalone tools.

We also observed a series of wargames run by NATO's SAS-151 group. We were asked by the group to provide an analysis of IFC use in one of those games, the results of which are also discussed in this chapter. The information used in this analysis was garnered by members of the RAND team who observed game events from different teams' vantage points, documenting both their game moves and the underlying rationale for those moves as expressed during team discussions.

How and Why to Integrate IFCs into Wargames

Why Game IFCs

Wargames that integrate IFCs could be useful for a number of purposes, including generating insights on decisionmaking and perceptions regarding IFCs, supporting IFC-related innovation, and socializing IFCs across DoD. Studying IFC-related decisionmaking is a particularly apt use for wargames because asking players to make decisions given a problem or specific context is a key characteristic of almost every wargame. This means that games provide opportunities to confront players with the decisions researchers wish to explore and collect rich data on how players grapple with them. For example, a game in which players have opportunities to use IFCs could generate insights into how players think about IFCs—are they confused by the capabilities or associated concepts? Do they view them as valuable given the game's context? Are their decisions affected by expectations about their effects or escalation risks? When and why do they choose to employ or not employ IFCs?

Wargames can also be useful for supporting innovation. Games involving IFCs could be used to explore how military personnel might employ IFCs, including potential tactics, CONEMPs/CONOPs, and ways for integrating IFCs with lethal weapons or other IFCs. Grounding the use of IFCs in the context of a game, particularly one involving an adversary, also allows exploration of their effectiveness in specific situations, as well as exploration of potential responses to adversary use of IFCs or IFC countermeasures. Depending on the format and purpose of the game, the data generated could suggest areas for future IFC development, highlight ways in which IFCs could better meet warfighter needs, or provide insight into logistics, maintenance, and other support requirements.

Because good wargames are engaging experiences that often invite players to grapple with scenarios, problems, and capabilities they do not encounter on a day-to-day basis, games can also be effective vehicles for socializing new concepts or capabilities. This could be particularly valuable for IFCs because they lack widespread visibility across DoD. Exposing personnel to IFCs in games could create broader awareness of both their capabilities and their potential utility in certain situations (such the vignettes discussed in Appendix C), potentially lowering barriers to IFC adoption when players have opportunities to use them in the real world. Wargames could also be beneficial to organizations that already use IFCs, socializing them to innovative capabilities and CONOPs/CONEMPs or other organizations' approaches to IFCs.

Current State of Integration into Games and Challenges That May Affect Integration

Non-Lethal Weapons

Wargames involving IFCs—and particularly NLWs—are currently rare. While there have been efforts to include cyber and EW in wargames, none of the 26 wargaming experts we interviewed had personally observed NLWs played in a DoD game, although one had heard of such a game happening. We observed NLWs used in a series of games run by the NATO SAS-151 group, with participation from DoD personnel; however, SAS-151 was specifically focused on studying the full range of IFCs (NLWs, EW, cyber, and IO). Interviewees indicated that NLWs appear somewhat more often in commercial wargames, but these games are intended as entertainment—designed primarily to be engaging and easy to play, not to accurately portray capabilities and their effects.

Despite the paucity of wargames including NLWs, many of our interviewees believed that opportunities exist for their integration; however, there are a variety of challenges in doing so. First, wargame adjudication typically focuses on attrition of forces, whereas NLWs often have psychological impacts on such things as morale and will to fight. This means that current adjudication methods are ill-suited for adjudicating NLW usage. Furthermore, many newer NLWs are in development and lack extensive field testing, making development of mechanisms that accurately reflect their effects difficult. In addition, many DoD games are operational-level games focusing on conventional, high-intensity conflict. Although JIFCO is attempting to expand usage of NLWs within DoD, NLWs have not traditionally played a role in this context, making their exclusion in related games unsurprising. This may be difficult to change because there are other capabilities with more traditional applicability to high-end conflict—such as space capabilities—that are also at the beginning stages of integration into games. The inclusion of these capabilities may take precedent over integrating NLWs.

Cyber, Electromagnetic Warfare, and Information Operations

Other IFCs, such as cyber and EW, are becoming more common in operational-level games, but they face their own set of challenges. Unlike NLWs, these capabilities are often highly classified, meaning that their representation in games that are unclassified or even at low levels of classification is often notional, with significant ramifications for the fidelity of wargame results. Adjudication of cyber and EW impacts is further complicated by the fact that these capabilities are often highly specific to the systems they are targeting, limiting how well their effects can be abstracted into game mechanics. In addition, their effects can be less predictable than those of conventional weapons.

IO is rarely included in wargames beyond participants' mutual posturing toward one another; while the challenges faced are similar to those of gaming cyber and EW, it has been less of a priority within DoD.[1] The impacts of IO campaigns are similarly unpredictable, and adjudication typically relies on broad assumptions about how well a team can communicate messaging, to what degree such messaging resonates with the target population, and how the messaging actually shapes behavior or will to fight. This uncertainty about IO effects means that games that do include IO often handle it narratively. One of the recent SAS-151 games focused specifically on IO and used a novel crowd-based method for adjudicating the impact of messaging, but that game was very much an exception to current practice.

How to Effectively Integrate IFCs into Games

Generating a Scenario Based on Objectives

IFCs are more suitable for some real-life situations than others; this is likewise true for wargames. As described in Chapters Two and Three, IFCs can broadly help with managing escalation, avoiding collateral damage, and enhancing lethal capabilities. Games that encompass one or more of those concerns could offer opportunities to integrate IFCs. For example, IFCs would be a natural capability to include in games where players are operating in the vicinity of civilians, hostages, friendly forces, or sensitive infrastructure (e.g., nuclear power plants or chemical weapon storage facilities). They could also be useful for games where competition or crises have yet to transform into full-scale hostilities and managing escalation is a primary concern for players as they try to accomplish their objectives. Whatever scenario is chosen should be meaningful for reasons other than the opportunity it provides to integrate IFCs; players can grow frustrated and disengaged if a game seems like nothing more than a technology showcase.

IFCs will likely be more straightforward to include in tactical-level games than operational- and strategic-level games. Indeed, most of our interviewees had difficulty envisioning operational- or strategic-level games including IFCs, particularly NLWs. While this does not mean they cannot be played, aggregating the tactical-level effects of IFC use will likely reduce the fidelity with which their effects are represented in the game. It may also make more sense to roll their impacts into the representation of unit effectiveness rather than explicitly gaming them at the capability level. This could be done by feeding the results of multiple tactical games into the development of related operational and strategic games.

A game's objectives play a role in determining at which level of conflict a game should be played. For example, tactical-level games could be used in the refinement of TTPs, while operational ones could be used to shape CONOPS. Either type of game would be designed to spur innovation, but designing an operational game that effectively explores innovative tactics would be difficult. If a game's objectives would be best met by gaming multiple levels of conflict, it is generally advisable to run multiple separate games, each at a different level of conflict, rather than one game attempting to span multiple levels. The difference in the timescales relevant at different levels of conflict can be difficult to reconcile when playing at, for example, the tactical and operational levels concurrently.

[1] One notable exception is the Marine Corps Information Operations Center Information Warfighter Exercise (IWX), which is held one to two times a year and is designed to provide training on IO. A RAND tool describes the rule set used in the 2020 IWX cycle (Paul et al., 2021).

Introducing IFCs to Players

Introducing new capabilities in wargames is fairly common within DoD. When doing so, players' first impressions of the capabilities and of the game itself are critical for maintaining engagement and allowing players to incorporate the new capabilities into their decisionmaking. Maintaining credibility, while always important, is particularly vital for games intended to socialize IFCs, because they rely on player buy-in to achieve their core purpose. If players believe a game is designed to portray IFCs in an unduly flattering way, they may become frustrated.

There are a variety of methods for successfully introducing new capabilities, with the following provided as a sample, not an exhaustive list. First, players should be given background information on the capabilities they are expected to use, including their effects, potential CONEMPs, and relationships to other capabilities and systems (e.g., C^4ISR capabilities or the logistics system).[2] Clearly explaining why an unfamiliar capability is expected to have certain effects is particularly important, because players may balk at effects that seem "magical" or otherwise too good to be true. Physical handouts, such as capability cards outlining the key characteristics of relevant IFCs, can serve as useful references for players as they make decisions throughout the game. Second, it can be helpful to familiarize players with capabilities in advance, perhaps through a short practice game turn that demonstrates how a capability might be used. This empowers players to better integrate a new capability into their decisionmaking rather than ignore it in favor of more familiar capabilities. Finally, if a game is concerned with when and why players use a given capability, players should be given the same incentives (e.g., rules of engagement, policy considerations) to use that capability that they would have in reality. This can help mitigate potential overuse by players who assume that, because the game designers have included a new capability in a game, they expect players to use it as much as possible.

When considering the type of IFC information that will be provided to players, as well as which methods will be used to familiarize players with IFCs, it can be helpful to consider the decisionmaking roles that players are being asked to take on during the game. In wargames, players are often not playing themselves within the fiction of the game scenario. In a tactical game, they may be taking on the role of platoon commanders making decisions about employment of specific IFCs by soldiers under their command; in a strategic game, they may be acting as National Security Council members advising the President on responses to an international crisis involving use of force against civilians. The type of information these decisionmakers would have on IFCs in reality varies dramatically, and it often makes sense for the information given to the players to reflect that. Players in a tactical game may need specific information on the performance of each IFC available to them on capability cards. Players in a strategic game may not require capability cards, instead benefiting from information on public opinion regarding IFCs in general.

Designing Game Mechanics and Adjudication Processes

Most wargames involve some sort of adjudication of player decisions based on game mechanics and underlying models of the phenomena explored in the game. Sometimes game adjudication is quite detailed, relying on physics-based models of the phenomena explored in the game; sometimes it is very high-level, relying solely on subject-matter experts. Regardless, it is vital that a game's structure, rules, and adjudication be free of both real and perceived bias. The former influences the reliability of a game's results, while the latter reduces players' willingness to engage in the game, as well as the trust others have in the game results.

Credible adjudication of IFC use in games requires conducting background research to build well-grounded explanations for IFC effects, particularly for NLWs. That said, IFCs vary widely in the amount of available data on their effects, which affects the type of adjudication that be done. Building detailed models

[2] Some of this information may be eliminated in player resources or orientations if the purpose of the game is to elicit it; however, it can still sometimes be useful to provide examples as a starting point.

of NLW impacts requires a lot of data, lest the model results provide a false sense of precision. These data sets could include testing data on NLWs' physical effects, research on NLWs' psychological impacts, data on historical NLW usage, research on crowd or group dynamics, and other modeling and simulation work. For example, data on how the effects of the Active Denial System (ADS) are influenced by range, environmental conditions, the demographics of the exposed population, and other factors can inform who is affected. How those affected individuals are likely to behave can then be assessed based on exercise data, psychological insights and modeling, and any available real-world experiences. Although some NLWs have not yet been employed in operational environments, available data regarding the effectiveness of other systems in managing standoffs, dispersing crowds, or other contexts may be used as a rough proxy. For example, historical incidents at sea where acoustic hailers were used to warn and discern intent can contribute to some assessment of how people might react to other types of NLWs in similar situations.

If data sets along these lines do not exist, less detailed, rough qualitative adjudication may be more appropriate. In all cases, but particularly when minimal data sets are available to inform adjudication, it is important to remember that games are typically more useful for identifying potentially fruitful avenues of inquiry than providing definitive answers or predictions. Thus, expectations for the type of information a game will provide should be tempered.

Adjudication in the absence of detailed models has a long history in wargaming; the following are a few potential methods that could be used for this (Perla, 1990). First, adjudication could focus on the effects of IFCs instead of the process by which they create those effects. For example, process-based adjudication might note that, taking the specific situation in the game move into account, an ADS creates an intense heating sensation among people in its beam, which in turn is likely to cause less-motivated individuals to run away, potentially scaring away other people in the area as well. Effects-based adjudication would simply note that use of an ADS typically compels people to move out of the way. Effects-based adjudication could be particularly useful for handling cyber and EW capabilities in light of the previously described challenges faced in adjudicating their effects. Second, IFC effects can be described as changing something in one direction or another without precisely quantifying that change. For example, use of an IFC might be said to decrease a unit's cohesion and will to fight. Depending on the IFC models available, reducing the granularity of the adjudication results in this way may more appropriately reflect the quality of the models than providing numerical values does. Finally, discussion-based adjudication can be used to elicit player knowledge of IFC effects. This style of adjudication is often interactive—players are allowed and even encouraged to push back on results based on their own expertise, helping to refine the representation of IFC effects in the game. Note that games using this type of adjudication run the risk of devolving into aimless group discussions, so it is important to insist that players take specific actions during each game turn and make explicit arguments for why those actions would be effective in the context of the game.[3] Even when using discussion-based adjudication, it may be useful for the adjudication team to rely on data on relevant IFC usage to the extent that is possible. If players argue that IFC usage in the game will have different impacts than those seen in experiments, historical use cases, etc., they can be asked to explicitly state why they expect that divergence to occur.

There are a few other important considerations when designing game mechanics, regardless of the adjudication method chosen. All games are to some degree an abstraction of reality. Game designers have to consider what aspects of reality to represent in their games, and players have to decide what aspects of reality (and of the game) to consider in their decisionmaking. When making decisions during a game, players tend to ignore anything without consequences in the context of that game, even if it is important in reality. This means using or not using IFCs in a game has to have consequences in order for IFCs to matter to the players, and these consequences have to be integrated into the broader course of events in a game, with some impact

[3] For more information on games using discussion-based adjudication, see Rothweiler (2017) and Jones (1985).

on whatever the players are trying to accomplish. It is important that these consequences be relevant at both the level of conflict and timescale represented by the game. Games should also be designed to account for second-order effects of IFC usage, including target responses and introduction of IFC countermeasures. IFCs target thinking individuals, and, whether adversaries or bystanders, they will react in ways that reflect that.

Selecting Players

Because games often study human decisionmaking, whether directly or indirectly, great care should be taken when choosing players. While financial or scheduling realities can make assembling the ideal group of players difficult, the players chosen should bring the appropriate expertise and perspectives required to play the roles they will be assigned in the game. A more thorough handling of this topic can be found in works like *The Art of Wargaming* and *Wargame Pathologies*, but our interviewees also provided the following insights for games exploring IFC TTPs or CONOPS.[4] As previously noted, it can be helpful to provide players with examples for how IFCs might be used, and this is even true for games exploring TTPs or CONOPS. The skillsets and mentalities required to conduct effective wargaming and creative innovation do not always overlap, so players with a lot of experience in wargaming but little experience in capability-related innovation can benefit from having provisional TTPs and CONOPS to adapt during a game, rather than being asked to develop new ideas from nothing. Otherwise, they may simply wedge the new capabilities into old TTPs and CONOPS. Inviting innovative players with little wargaming experience also has pitfalls. Participating in a wargame requires a willingness to engage with the scenario of the game and make decisions within its bounds while knowing that it is an imperfect model of reality. Regardless of their expertise, players who do not arrive with a willingness to engage in the gaming experience may not provide useful insights.

Modeling and Simulation

M&S can provide insights into IFC effects both as a standalone activity and as an input into wargames. M&S are particularly useful in quantifying or predicting outcomes—something wargames are ill-suited for. In particular, they could help build a better understanding of IFC effects that differ from those of their lethal counterparts, including their psychological impact on individuals and effect on group dynamics. Such models should incorporate insights from field testing, historical data, and research on psychology and group dynamics into their inputs, assumptions, and algorithms. Because human behavior is not consistent or wholly predictable, they should account for variability and uncertainty.

For most purposes, it likely makes more sense to build new M&S tools for IFC research than to attempt to integrate IFCs into existing tools, particularly at the tactical level. All models make assumptions, and some may not be explicit, making them hard to discern, much less modify appropriately to account for IFCs. In addition, many models and simulations are attrition-based—focused on the physical damage dealt by lethal capabilities. Tailoring these tools to model psychological effects could be time-consuming and expensive, and modeling only those IFC effects that can be represented as physical attrition of forces may inadequately capture IFCs' true utility.

Building new M&S tools allows them to be tailored to the analyses they are intended to support. For example, researchers at the Naval Postgraduate School and JIFCO have developed the Workbench for refining Rules of Engagement against Crowd Hostiles (WRENCH) model, which is specifically designed to explore the impact of NLWs (Crowd Dynamics Modeling Group, Naval Postgraduate School, undated). When developing models, the level of complexity in inputs, assumptions, algorithms, and outputs should be mini-

[4] Perla, 1990; Weuve et al., 2004.

mized as much as possible without unacceptably decreasing the tools' accuracy. This makes them easier to use, interpret, and update.

Because research on the effects of IFCs is, in many cases, still ongoing, it may be unclear which inputs and assumptions to use. This means that it might be helpful to conduct parametric analysis of the sensitivity of M&S outcomes to different inputs and assumptions. It may be feasible to integrate the results of such parametric analyses of IFC effects into higher-level M&S tools, say at the campaign level, but would be dependent on the flexibility of the model. In general, all-encompassing campaign models are an exception to the rule that it is generally more desirable to create IFC-specific models. Replicating large-scale existing DoD models that include numerous warfare areas so that they can include IFCs would be cost-prohibitive and would require lengthy accreditation processes. Rather, campaign models can incorporate findings from purpose-designed IFC models at the tactical and operational levels: For example, forces' effectiveness can be reduced, or their response timelines protracted, due to the other side's use of IFCs.

As previously noted, M&S can provide useful inputs for wargames and are particularly necessary for games using detailed adjudication of IFC effects. In such games, they provide a credible basis for adjudication, ensuring that IFC effects don't "smell like magic" to the players.[5] That said, M&S are best used to generate outcomes for a range of potential inputs before a game is executed, with a summary of the results used for adjudication during the actual game. M&S tools can take a long time to set up and run, so attempting to update and run the tools after every game move can be impractical.

Observations from a NATO Wargame on IFCs

Game Context and Scenario

We observed a series of NATO wargames focusing on IFCs, providing analysis for the final game in the series. In this game, Blue forces attempted to evacuate civilians and personnel associated with host-nation forces (e.g., family members of military personnel) from a friendly host country being invaded by Red, who sought to capture the civilians to gain leverage over the host nation. Successfully evacuating the civilians required moving them from an inland base to the coast, where they could be transferred to Blue ships. Host-country citizens who sympathized with Red's goals attempted to prevent the civilians (primarily transported by bus) from reaching the coast, while an adversary armored convoy attempted to reach the coastal point of embarkation before the civilians either arrived at that location or could be completely transferred to Blue vessels. Two rounds of the game were completed, one where Blue forces had existing IFCs and one where they had advanced IFCs. Red forces had access to only existing IFCs in both games. Our observation of this wargame provided insight into both the use of IFCs and into integrating IFCs into wargames.

Key RAND Findings from the Wargame

Findings on NLW Usage

During the game, Blue players adopted NLWs enthusiastically, using them to repel militia members attempting to impede buses carrying evacuees to the evacuation point. They also used IFCs to delay Red armored forces trying to reach the evacuation point before the evacuation could be concluded. Although NLWs didn't succeed in stopping the armored forces completely, they slowed them down, buying additional time for the evacuation to proceed and for Blue to find additional options to respond to the situation. That said, the game highlighted the necessity for considering potential NLW countermeasures, which may be available even to

[5] Interview with RAND Corporation staff member, Arlington, Va., August 20, 2021 (non-attributional interview).

nonmilitary forces, although NLWs could still be useful in imposing costs and demonstrating resolve even if their effects are weakened. Exploration of NLW countermeasures should also include consideration of how those countermeasures could be countered in turn.

The game also generated useful insights into the dynamics of escalation in situations involving both NLWs and lethal weapons. In general, NLWs were seen as less escalatory than lethal weapons, and even non-lethal use of traditionally lethal weapons bumped escalation up to a different level of intensity. The game suggested that this difference in the perceptions of lethal and non-lethal capability use may be due in part to the higher risk of collateral damage from lethal systems, even when used with non-lethal intent. However, this is not to say that using NLWs is always non-escalatory; in a previous SAS-151 game playing out a maritime crisis, we observed use of an ADS framed as an "act of war" and used as justification for use of lethal fires by the Red team. Regardless of the lethality of capabilities used, we observed that escalation by one party to a conflict or crisis was perceived as opening up escalation as an option for other parties. In the absence of powerful restraining factors, there was a natural tendency for both sides to escalate, even if only using NLWs.

We also observed opportunities for future investment; the game results suggested that there would be potential utility in developing a more compact, less power-hungry, more mobile ADS as a means for slowing or stopping the movement of armored vehicles. ADS was critical in a number of contexts—for example, clearing people from roads used by the evacuation convoy—but early demonstration systems are not very mobile due to large mass, volume, and power requirements. Inhibiting armor without resorting to lethal force is challenging but could be critically important in managing crises without causing unwanted levels of escalation. NLWs used for this purpose would likely need to be integrated with other measures to achieve a high degree of effectiveness—otherwise, they could be circumvented relatively quickly. In the context of the game, NLWs capable of more effectively slowing or stopping armor on paved roads would have been particularly useful.

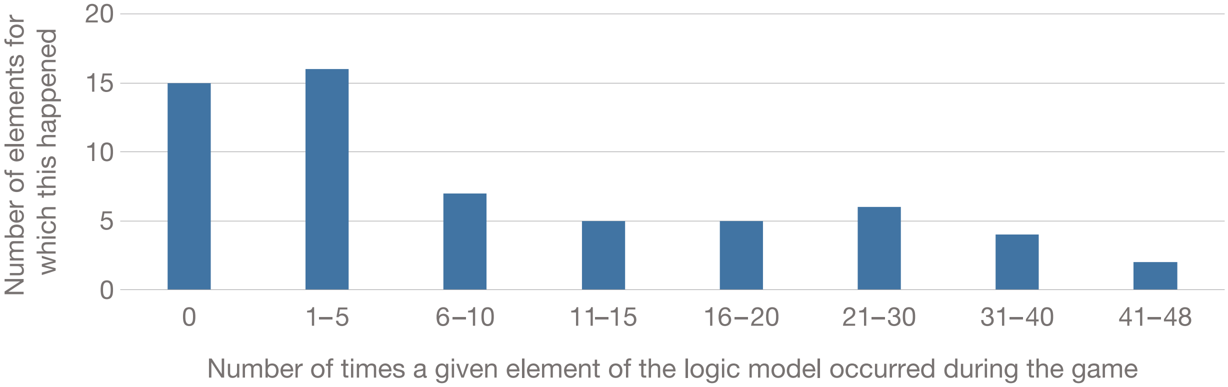
Findings on Gaming IFCs

The SAS-151 game also yielded useful insight into introducing IFCs, particularly NLWs, to wargame players. Despite preparatory sessions and the availability of capability cards describing IFC effects, participants were often confused about the specific capabilities of their NLWs and which platforms could host them, as well as about each team's order of battle. For example, they sometimes assumed that directed-energy weapons could produce effects despite physical obstructions between them and their targets. The participants in this game were generally already familiar with NLWs, so this issue may be more pronounced in games where the capabilities are new to the people playing. Player understanding of NLWs and orders of battle could potentially be improved by conducting initial briefings or assigning members of the control cell to rotate through the teams providing factual information. That said, there could be contexts in which player uncertainty is reflective of real-world conditions and leaving said uncertainty unresolved could contribute to a game's objectives. In reality, many military personnel will likely have a less thorough understanding of the specific capabilities of NLWs than they do of traditional lethal systems, particularly for recently fielded NLWs or other IFCs, such as cyber and electronic warfare.

Application of Logic Model to Game

After observing the SAS-151 game, we analyzed all instances of IFC usage in the game to identify how the use of IFCs overlapped with the NATO-centric logic model described in Chapter Three. After tabulating the number of times IFC usage contributed to each element of the logic model, we found that, over the course of the game, IFC use contributed at least ten times to 23 of the 60 activity, output, and outcome elements. This engenders confidence in the validity of the logic model. Figure 4.1 shows the distribution for the number of times IFCs contributed to each logic model element during the game.

FIGURE 4.1
Distribution of Logic Model Element Recurrence



The elements of the logic model that were most relevant to the SAS-151 game are listed below. All elements listed came up in the context of IFC usage at least ten times, with bolded elements recurring at least 25 times. They are color coded in the same way as the elements shown in Figure 3.1: Purple indicates elements applicable primarily to NLWs, orange indicates elements applicable primarily to IO, and green indicates elements applicable to all types of IFCs (NLW, IO, EW, and cyber).

Activities

- Elements that primarily relate to NLWs
  - **Affect mobility: Slow, impede, halt, prevent from approaching or leaving, redirect, disperse, impel departure**
  - Compel/tactically deter: Convince others to take or not take specific actions
  - Incapacitate infrastructure/materiel
- Elements that primarily relate to IO
  - Disseminate information to inform and persuade
  - Disseminate information to affect adversary perceptions and assessments
- Elements that relate to NLWs, IO, EW, and cyber
  - Deceive, distract, disorient, or confuse
  - Degrade, disrupt, and destroy adversary systems and C^4ISR

Outputs

- Elements that relate to NLWs, IO, EW, and cyber
  - **Effectively responded to situations despite constraints**
  - **Increased options for engaging targets**
  - **Reduced risk of exceeding ROE or Laws of War**
  - **Reduced adversary options and imposed costs**
  - Gained time/distance before deciding to take lethal action
  - Reduced risk of NATO, partner personnel casualties
  - Reduced risk to NATO systems or facilities
  - **Conserved and augmented lethal capabilities**
  - Reduced NATO tactical costs (broadly defined)

- Elements that primarily relate to IO
  - Affected perceptions, decisionmaking, and behavior of adversary personnel
  - **Influenced perceptions, decisionmaking, and behavior of populations**

Outcomes

- Elements that relate to NLWs, IO, EW, and cyber
  - **Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts**
  - **Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks**
  - **Delayed, degraded, disrupted, manipulated, or precluded adversary actions**
  - Reduced effects of adversary attempts to delay, degrade, disrupt, manipulate, or preclude NATO and partner actions
  - Projected power or demonstrated capabilities using IFCs

Key Takeaways

Through their immersive, interactive, and competitive nature, games can allow players to grapple with new challenges and provide unique insights into human behavior. Because of this, including IFCs in wargames could provide valuable opportunities to study IFC-related decisionmaking and allow a wide variety of players to learn more about IFCs. Successfully integrating IFCs into gaming will require designing games in ways that address their non-attritive, often psychological effects in appropriate contexts and levels of conflict. This is often challenging, because IFC effects are generally more difficult to characterize than those of other types of weapons. Most wargame adjudication focuses on which items have been physically destroyed or incapacitated, whereas IFCs result in more subtle effects. IO efforts and some NLWs primarily affect human psychology to shape behaviors, while EW, cyber, and select NLWs impede the functioning of machines, generally without destroying them.

Overall, we found that there is a lot of potential value in wargaming IFCs, but there are a number of challenges that will need to be overcome in order to do this effectively. Success will require ensuring that players are familiar with the IFCs that are being used and have a clear understanding of the consequences of their uses, as well as any second-order effects. For example, a wargame may involve the use of eye-safe laser dazzlers that create glare to impair, annoy, and distract. In a hypothetical standoff with forces from a rival nation in a third country, laser dazzlers could help to warn the other side to back away from a confrontation, helping to defuse the situation without recourse to lethal force. On the other hand, subjecting them to intense glare without employing complementary means of communication (such as acoustic hailers or radios) could potentially escalate the situation, if the other side misinterpreted what was happening. The wargame's creators would need to describe the precise effects of these systems, ensuring that participants clearly understand that the laser dazzlers do not wholly incapacitate their targets but can affect their behavior. Participants would also need to be aware of potential adversary countermeasures, such as the use of specific types of goggles that can diminish the effectiveness of laser dazzlers.

Likewise, the contexts, scenarios, and levels of conflict of the wargame need to be crafted to elicit appropriate insights regarding the utility of these systems. The appropriate use of IFCs in a U.S. standoff with forces from a rival nation depends heavily on the physical environment. Laser dazzlers are line-of-sight weapons, so, in an urban environment, an adversary with indirect-fire capabilities may try to counter them by getting behind buildings and having uncrewed aircraft provide situational awareness. The laser dazzlers could be directed at the uncrewed aircraft to impair their sensors, but the psychological effects would be different: A human's response to a blanked-out screen is not necessarily the same as the response to directly experiencing a beam of glare. All of these dynamics would be very different in an open desert with minimal cover, and there would be far fewer risks of collateral damage by either side. A maritime standoff that began with a freedom-of-navigation exercise being impeded by another nation's vessels trying to claim sovereignty would be different not only tactically, but also because it would be imbued with a greater level of strategic significance. Wargame designers need to take all these various considerations into account.

Integration of NLWs into DoD wargames has been extremely rare; while other IFCs, including cyber and EW, have been more commonly integrated into games, this has rarely been without difficulty. Two common issues in doing so are the extremely high classification of the details of many cyber and EW capabilities and a high degree of uncertainty about the effects of certain technologies that requires game designers to make bold assumptions.

Overcoming the current barriers to integrating IFCs in gaming will require developing credible methods for adjudicating their effects. This could be aided by a combination of research on psychology and group dynamics, test data, historical usage data, and M&S. Regarding M&S, it will likely be a better choice to develop new M&S tools that are tailored for IFCs than to rework existing models to account for IFC effects, particularly at the tactical level. While these tools can play a role in supporting wargames, they could also be useful for IFC research on their own. Indeed, they are more appropriate than wargames for quantifying or predicting outcomes of IFCs use.

Our observations of the SAS-151 game suggested that more analysis is needed regarding action-reaction dynamics when IFCs are used, the impact of IFCs on escalation, and the extent to which countermeasures against IFCs influence their impact on adversary behaviors. Regarding adversary countermeasures for IFCs, the fact that IFC effects can be degraded does not make them useless, because they can still increase the time and space Blue forces have to act when their effects are reduced. This does mean, however, that potential countermeasures and even counter-countermeasures should be considered when assessing the potential impact of IFCs.

CHAPTER FIVE

Conclusions and Recommendations

Conclusions

The DoD Logic Model Remains Robust

By updating the strategic goals for the DoD-centric version of our logic model to reflect the goals from the 2022 NDS, we found that the logic model that we created for our previous study continues to be relevant, as the same set of activities, outputs, and outcomes from that logic model strongly supports the strategic goals we derived from both the 2018 and 2022 NDSs. These remain the elements of the logic model that should be focused on when assessing the impacts of NLWs. Notably, the five key IFC outcomes in the logic model were

- competing effectively and demonstrating resolve while managing escalation
- conducting operations in environments that would otherwise be too risky
- avoiding alienation of host-nation populations, forces, and governments
- enhancing perceptions of U.S. forces, both domestically and internationally
- increasing cooperation with partners.

The NATO Logic Model Demonstrates the Utility of the IFC Concept

When we expanded the logic model to encompass the more expansive definition of IFCs for NATO, we found that many of the elements of the original logic model were also applicable to IO, EW, and cyber. Going from activities, to outputs, to outcomes, the elements of each level of the logic model became increasingly applicable to the full spectrum of IFCs, rather than one in particular. This indicates that it makes sense to consider these technologies as a set of complementary capabilities. Once we completed a connectivity mapping, six activities, eight outputs, and seven outcomes were revealed to be particularly strongly linked to strategic goals. These 21 elements are the ones that should be emphasized when evaluating the impact of IFCs in a NATO context.

We identified 153 metrics to measure the new activities, outputs, and outcomes, and we added seven additional metrics to existing logic model elements that were applicable to the larger definition of IFCs to ensure that they measured all aspects of those capabilities. We found that nearly all of the metrics were good measures of their associated logic model elements, with 85 percent of the metrics rating high in terms of their validity. In terms of feasibility and timeliness, the quality of the metrics depended on the IFC that they were attempting to measure. Cyber metrics are comparatively quick and easy to measure. EW metrics are harder to measure because of uncertainty regarding how quickly and accurately electromagnetic emissions can be characterized. IO metrics are generally quite difficult and time-consuming to measure because they often involve assessing how human beings relate to and engage with information.

The 11 vignettes reveal that IFCs can be relevant in a wide range of potential NATO contexts, including during full-scale combat, and many of the potential uses of different types of IFCs are complementary and even synergistic. Overall, we identified diverse situations in which IFCs could benefit NATO, and our analysis indicates that the conception of NLWs, IO, EW, and cyber as belonging under a single IFC umbrella has value, insofar as they can contribute to each other's success. This indicates that it makes sense to consider these technologies as a set of complementary capabilities, integrating them under the IFC umbrella. The four areas also share a common challenge, namely that their impact is difficult to measure.

Integrating IFCs into Wargaming and M&S Is Valuable but Challenging

Overall, we found that there is a lot of potential value in wargaming IFCs, if it is done well. The logic model, metrics, and vignettes can aid in informing wargame design; this was demonstrated in a NATO wargame on IFCs. As was discussed above with respect to potential scenarios involving the use of laser dazzlers in standoffs with rival powers, success will require a careful selection of the contexts, scenarios, and levels of conflict; ensuring that players are familiar with IFCs; and having a clear understanding of the consequences of their impact, as well as any second-order effects. We also found that integrating IFCs into M&S is likely best accomplished by developing new tools rather than attempting to fit IFCs into existing tools that were designed with lethal weapons in mind. This is particularly true when it is important to consider the psychological effects of IFCs.

Wargames are useful for gaining insights into human decisionmaking and providing opportunities for players to deeply engage with IFC technologies. To create an environment where this is possible, the game must be thoughtfully designed, particularly when incorporating the psychological impacts of IFCs, and have credible adjudication, which is where custom-designed modeling and simulation tools can provide key inputs.

Recommendations

Our overarching recommendations are as follows:

- **Use the updated DoD-centric logic model, together with the still-relevant vignettes and metrics described in the previous report, to help measure, document, and communicate the impact of NLWs within DoD.** The logic model provides a structure, now connected to the strategic goals of the 2022 NDS, to clarify how the activities that NLWs perform contribute to ultimate DoD aims; we have documented which elements of the logic model are most important in that regard. Measuring the values of metrics associated with those elements in real-world operations, exercises, and wargames can provide hard data with which to evaluate the impact of NLWs. The vignettes provide examples of NLW usage that can inform discussion throughout DoD, and they also serve as a basis for wargames that further elucidate the impact of NLWs.
- **Use the NATO-centric logic model, metrics, and vignettes to help measure, document, and communicate the impact of IFCs within NATO.** All the points in the preceding bullet also apply in a NATO context, using the logic model, metrics, and vignettes that are tailored to NATO's needs. Those NATO-centric items both address NATO strategic goals and include all four types of IFCs (NLWs, IO, EW, and cyber).
- **Use aspects of the NATO-centric logic model, metrics, and vignettes to help shape DoD's development of the IFC concept.** DoD does not yet have a doctrinal definition of *intermediate force capabilities*. However, DoD personnel can use the NATO-centric materials that include NLWs, IO, EW, and cyber to help to think through how these types of IFCs interact with one another, contributing to development of an integrated, DoD-wide IFC concept. Only the NATO strategic goals need to be excised from consideration; the rest are still relevant to DoD.

- **Invest in M&S to support IFC wargames.** The accuracy of game results is predicated on having sufficient data regarding the effects of IFCs, from experiments, modeling, exercises, and/or real-world operations. Because so much of the impact of IFCs (particularly NLWs) is psychological, understanding how different participants react to IFC usage can be valuable—e.g., how IFC usage can escalate or de-escalate situations, whether used alone or in combination with lethal weapons. Purpose-designed M&S that enable characterization of the psychological and other nonkinetic effects of IFCs can provide valuable insights on its own, and can also contribute to adjudication of wargames involving IFCs.
- **Conduct wargames in which IFCs play an integrated role.** While NLWs have almost never been professionally wargamed, and wargaming of other IFCs has often involved heroic assumptions, there is value in doing so. Integrating IFCs into wargames can provide insights on how IFCs could be used, their effectiveness in different contexts, the impact of using them in concert with other systems, and many other items. Because games typically have a limited ability to predict quantitative values like effectiveness, game insights should be used to guide future lines of inquiry using other methodologies, rather than treated as final confirmation of IFC utility (or lack thereof). Wargames can also create awareness of IFCs among participants who might not previously have considered their utility. In conducting wargames that emphasize IFCs, we make three key recommendations:
  - Familiarize players with IFCs before the game and at its outset.
  - Ensure that the capabilities and effects of IFCs that are used in the game are supported by documentation, and that adjudication of their impact is credible.
  - Allow for second-order effects of IFC usage (such as changed behavior to avoid exposure to IFCs) and direct adversary countermeasures to diminish IFCs’ impact.

APPENDIX A

Connections Among Levels of the NATO-Centric Logic Model

As was mentioned in the body of the report, the 75 elements within the NATO-centric logic model make it too complex to convey all the connections among them in a single diagram. Merely displaying all 75 elements on a single page (as in Figure 3.1) requires a small font, one that would have to be dramatically smaller to show the 646 connections among them. Rather, in this appendix, we provide diagrams illustrating the connections between each pair of levels of the logic model, followed by tables that provide the details of the strength of connections among each of the elements in those levels of the logic model. As discussed in Chapter Two, and in our previous report, we characterized the strength of the connections between logic model elements on a three-point scale:

- 2: strong, unequivocal connection
- 1: limited, indirect, or conditional connection
- 0: no connection.

We assigned a level of connection for each of the elements in adjacent levels of the logic model, so between each activity and output, each output and outcome, and each outcome and strategic goal. While this analysis was subjective in nature and would be difficult for another group of analysts to replicate exactly, providing this information allows for traceability, and we offer it up for the sake of completeness. For the detailed tables in this appendix (Tables A.2, A.3, and A.4), the 0, 1, or 2 in each cell indicates the strength of the connection between the logic model elements in the associated row and column based on the scale described above.

Before we present the results for each of the pairs of adjacent elements of the logic model, we present Table A.1, which shows the numbers of strong and limited connections among the various levels of the logic model.

TABLE A.1

Numbers of Connections Among Different Levels of the NATO-Centric Logic Model

	12 Inputs to 17 Activities	17 Activities to 25 Outputs	25 Outputs to 18 Outcomes	18 Outcomes to 3 Strategic Goals
Maximum possible connections (multiplying the number of elements in each column)	204	425	450	54
Strong, unequivocal connections	204	109	88	26
Limited, indirect, or conditional connections	0	87	115	17
No connection	0	229	247	11

Input-to-Activity Connections

Because all the inputs have strong connections to the activities, and a diagram showing those connections would be too dense to read, we did not include one here. The important takeaway is that all inputs are important, supporting all activities; an absence of any one input—systems, doctrine, TTPs, etc.—would preclude the ability to effectively conduct any activity.

Activity-to-Output Connections

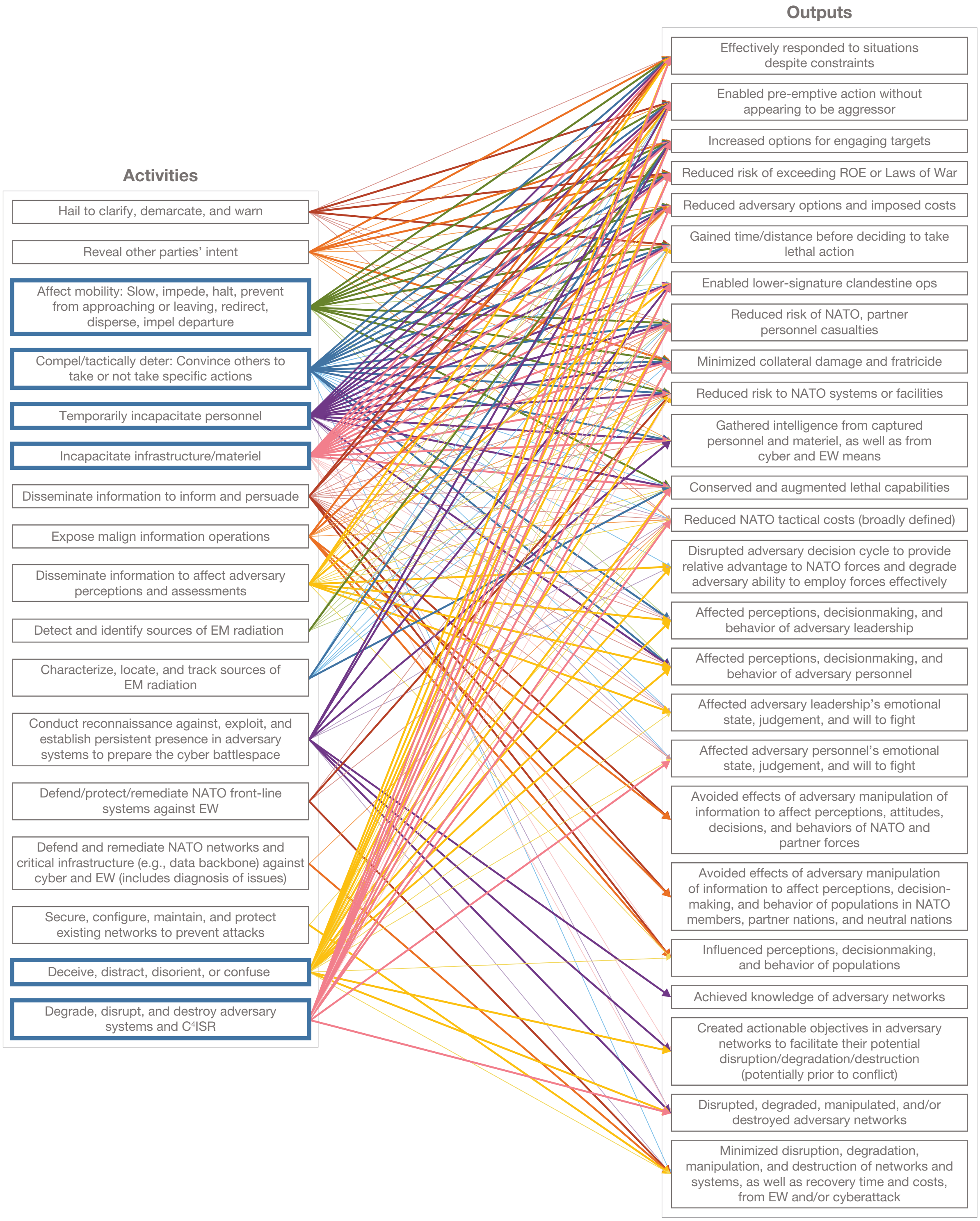
Figure A.1 shows the connections between the activity and output levels. Although the diagram is dense, it is also clear that some activities have more numerous strong connections to outputs than others do; the six with at least ten strong connections are surrounded by blue rectangles (and were earlier listed in Table 3.1).

In Table A.2, outputs are indicated by a letter, as follows:

A. Effectively responded to situations despite constraints
B. Enabled pre-emptive action without appearing to be aggressor
C. Increased options for engaging targets
D. Reduced risk of exceeding ROE or Laws of War
E. Reduced adversary options and imposed costs
F. Gained time/distance before deciding to take lethal action
G. Enabled lower-signature clandestine ops
H. Reduced risk of NATO, partner personnel casualties
I. Minimized collateral damage and fratricide
J. Reduced risk to NATO systems or facilities
K. Gathered intelligence from captured personnel and materiel, as well as from cyber and EW means
L. Conserved and augmented lethal capabilities
M. Reduced NATO tactical costs (broadly defined)
N. Disrupted adversary decision cycle to provide relative advantage to NATO forces and degrade adversary ability to employ forces effectively
O. Affected perceptions, decisionmaking, and behavior of adversary leadership
P. Affected perceptions, decisionmaking, and behavior of adversary personnel
Q. Affected adversary leadership's emotional state, judgement, and will to fight
R. Affected adversary personnel's emotional state, judgement, and will to fight
S. Avoided effects of adversary manipulation of information to affect perceptions, attitudes, decisions, and behaviors of NATO and partner forces
T. Avoided effects of adversary manipulation of information to affect perceptions, decisionmaking, and behavior of populations in NATO member, partner, and neutral nations
U. Influenced perceptions, decisionmaking, and behavior of populations
V. Achieved knowledge of adversary networks
W. Created actionable objectives in adversary networks to facilitate their potential disruption/degradation/destruction (potentially prior to conflict)
X. Disrupted, degraded, manipulated, and/or destroyed adversary networks
Y. Minimized disruption, degradation, manipulation, and destruction of networks and systems, as well as recovery time and costs, from EW and/or cyberattack

FIGURE A.1

Connections Between the Activity and Output Levels of the NATO-Centric Logic Model


Activities
Hail to clarify, demarcate, and warn
Reveal other parties' intent
Affect mobility: Slow, impede, halt, prevent from approaching or leaving, redirect, disperse, impel departure
Compel/tactically deter: Convince others to take or not take specific actions
Temporarily incapacitate personnel
Incapacitate infrastructure/materiel
Disseminate information to inform and persuade
Expose malign information operations
Disseminate information to affect adversary perceptions and assessments
Detect and identify sources of EM radiation
Characterize, locate, and track sources of EM radiation
Conduct reconnaissance against, exploit, and establish persistent presence in adversary systems to prepare the cyber battlespace
Defend/protect/remediate NATO front-line systems against EW
Defend and remediate NATO networks and critical infrastructure (e.g., data backbone) against cyber and EW (includes diagnosis of issues)
Secure, configure, maintain, and protect existing networks to prevent attacks
Deceive, distract, disorient, or confuse
Degrade, disrupt, and destroy adversary systems and C4ISR
Outputs
Effectively responded to situations despite constraints
Enabled pre-emptive action without appearing to be aggressor
Increased options for engaging targets
Reduced risk of exceeding ROE or Laws of War
Reduced adversary options and imposed costs
Gained time/distance before deciding to take lethal action
Enabled lower-signature clandestine ops
Reduced risk of NATO, partner personnel casualties
Minimized collateral damage and fratricide
Reduced risk to NATO systems or facilities
Gathered intelligence from captured personnel and materiel, as well as from cyber and EW means
Conserved and augmented lethal capabilities
Reduced NATO tactical costs (broadly defined)
Disrupted adversary decision cycle to provide relative advantage to NATO forces and degrade adversary ability to employ forces effectively
Affected perceptions, decisionmaking, and behavior of adversary leadership
Affected perceptions, decisionmaking, and behavior of adversary personnel
Affected adversary leadership's emotional state, judgement, and will to fight
Affected adversary personnel's emotional state, judgement, and will to fight
Avoided effects of adversary manipulation of information to affect perceptions, attitudes, decisions, and behaviors of NATO and partner forces
Avoided effects of adversary manipulation of information to affect perceptions, decision-making, and behavior of populations in NATO members, partner nations, and neutral nations
Influenced perceptions, decisionmaking, and behavior of populations
Achieved knowledge of adversary networks
Created actionable objectives in adversary networks to facilitate their potential disruption/degradation/destruction (potentially prior to conflict)
Disrupted, degraded, manipulated, and/or destroyed adversary networks
Minimized disruption, degradation, manipulation, and destruction of networks and systems, as well as recovery time and costs, from EW and/or cyberattack

NOTE: A thick, dark line means a strong, direct, unequivocal connection; a thin, light line means a limited, indirect, or conditional connection. Arrows emanating from a common source have the same color to make them easier for the reader to follow. A blue rectangle indicates an activity with strong links to at least ten outputs.

TABLE A.2

Strength of Connections Between Activities and Outputs

	Output																								
Activity	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Hail to clarify, demarcate, and warn	1	2	1	2	0	2	0	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Reveal other parties' intent	2	1	2	2	1	1	0	1	2	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Affect mobility: Slow impede, halt, prevent from approaching or leaving, redirect, disperse, impel departure	2	2	2	2	2	2	1	2	2	2	1	2	1	0	1	1	0	0	0	0	0	0	0	0	0
Compel/tactically deter: Convince others to take or not take specific actions	2	2	2	2	2	2	1	2	2	2	0	1	1	1	2	2	1	1	0	0	0	0	0	0	1
Temporarily incapacitate personnel	2	2	2	2	2	2	2	2	2	2	2	2	1	0	1	2	1	1	0	0	1	0	0	0	0
Incapacitate infrastructure/materiel	2	2	2	2	2	2	2	2	2	2	2	2	1	0	1	1	1	1	0	0	1	0	1	1	0
Disseminate information to inform and persuade	2	2	0	0	1	0	0	1	0	1	1	1	1	0	1	1	1	1	2	2	2	0	0	0	0
Expose malign information operations	2	0	0	0	2	0	0	1	1	1	0	0	1	0	0	0	0	0	2	2	2	0	0	0	0
Disseminate information to affect adversary perceptions and assessments	2	2	1	0	1	0	2	1	0	1	1	1	1	2	2	2	2	2	0	0	1	0	0	0	0
Detect and identify sources of electromagnetic (EM) radiation	0	1	2	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Characterize, locate, and track sources of EM radiation	0	1	2	0	0	1	0	1	1	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0
Conduct reconnaissance against, exploit, and establish persistent presence in adversary systems to prepare the cyber battlespace	0	2	2	0	0	0	2	0	0	0	2	0	1	1	0	0	0	0	0	0	0	2	2	2	1
Defend/protect/remediate NATO front-line systems against EW	0	0	0	0	0	0	0	1	0	2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	2
Defend and remediate NATO networks and critical infrastructure (e.g., data backbone) against cyber and EW (includes diagnosis of issues)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	2
Secure, configure, maintain, and protect existing networks to prevent attacks	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	2
Deceive, distract, disorient, or confuse	2	2	2	2	1	2	1	2	1	2	0	2	1	2	2	2	1	1	0	0	1	0	2	2	1
Degrade, disrupt, and destroy adversary systems and C^4ISR	2	2	2	2	2	1	2	2	2	1	0	2	2	0	0	0	0	0	0	0	0	0	0	2	0

Output-to-Outcome Connections

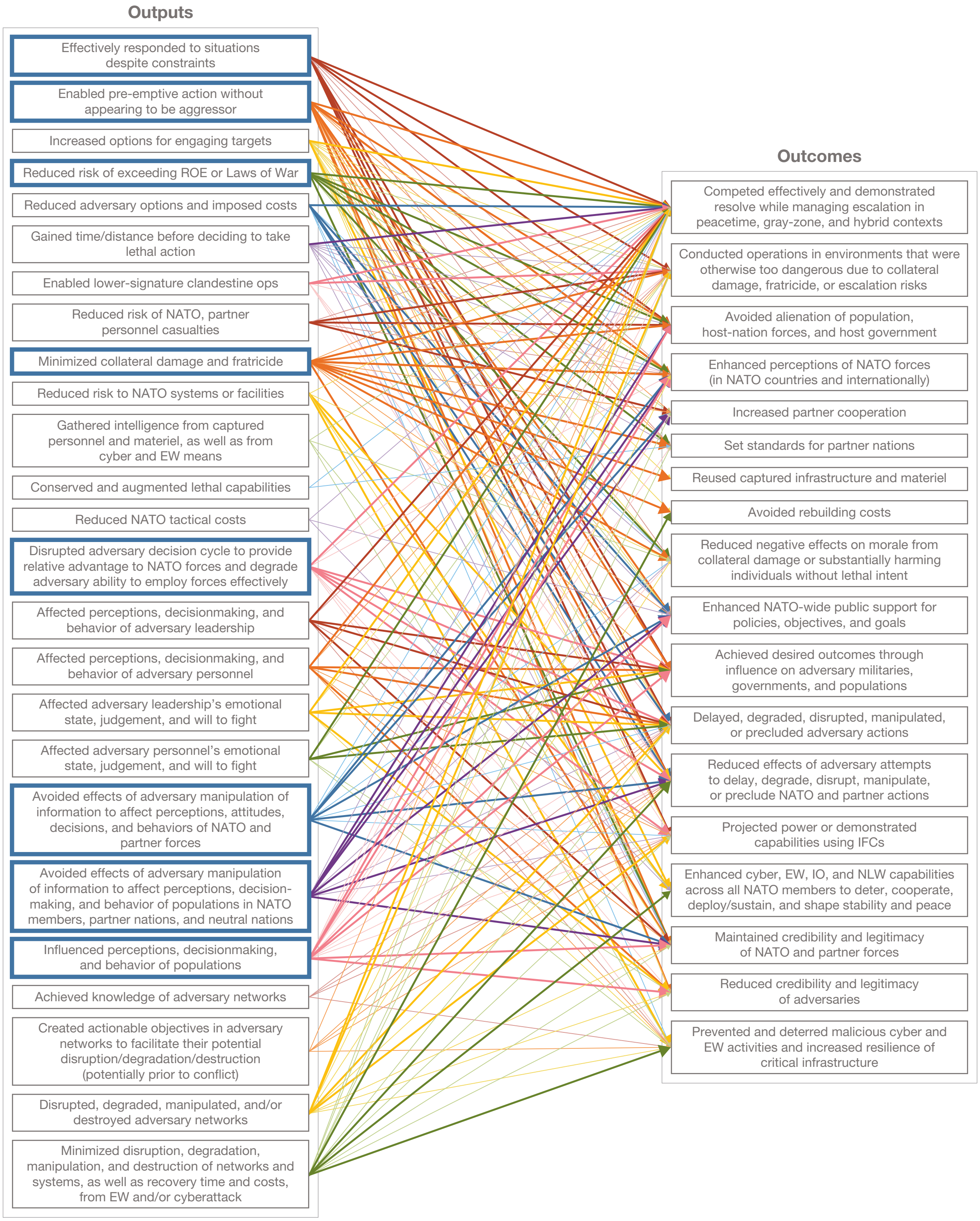
Figure A.2 shows the connections between the output and outcome levels. Again, while there are numerous connections, it also is visually evident that some outputs are better-connected than others. The eight outputs with at least five strong connections to outcomes, previously listed in Table 3.1, are surrounded by blue rectangles.

In Table A.3, outcomes are indicated by a letter, as follows:

A. Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone and hybrid contexts
B. Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks
C. Avoided alienation of population, military forces, and government in non-member states where NATO is operating
D. Enhanced perceptions of NATO forces (in NATO countries and internationally)
E. Increased partner cooperation
F. Set standards for partner nations
G. Reused captured infrastructure and materiel
H. Avoided rebuilding costs
I. Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent
J. Enhanced NATO-wide public support for policies, objectives, and goals
K. Achieved desired outcomes through influence on adversary militaries, governments, and populations
L. Delayed, degraded, disrupted, manipulated, or precluded adversary actions
M. Reduced effects of adversary attempts to delay, degrade, disrupt, manipulate, or preclude NATO and partner actions
N. Projected power or demonstrated capabilities using IFCs
O. Enhanced cyber, EW, IO, and NLW capabilities across all NATO members to deter, cooperate, deploy/sustain, and shape stability and peace
P. Maintained credibility and legitimacy of NATO and partner forces
Q. Reduced credibility and legitimacy of adversaries
R. Prevented and deterred malicious cyber and EW activities and increased resilience of critical infrastructure

FIGURE A.2

Connections Between the Output and Outcome Levels of the NATO-Centric Logic Model


Outputs
Effectively responded to situations despite constraints
Enabled pre-emptive action without appearing to be aggressor
Increased options for engaging targets
Reduced risk of exceeding ROE or Laws of War
Reduced adversary options and imposed costs
Gained time/distance before deciding to take lethal action
Enabled lower-signature clandestine ops
Reduced risk of NATO, partner personnel casualties
Minimized collateral damage and fratricide
Reduced risk to NATO systems or facilities
Gathered intelligence from captured personnel and materiel, as well as from cyber and EW means
Conserved and augmented lethal capabilities
Reduced NATO tactical costs
Disrupted adversary decision cycle to provide relative advantage to NATO forces and degrade adversary ability to employ forces effectively
Affected perceptions, decisionmaking, and behavior of adversary leadership
Affected perceptions, decisionmaking, and behavior of adversary personnel
Affected adversary leadership's emotional state, judgement, and will to fight
Affected adversary personnel's emotional state, judgement, and will to fight
Avoided effects of adversary manipulation of information to affect perceptions, attitudes, decisions, and behaviors of NATO and partner forces
Avoided effects of adversary manipulation of information to affect perceptions, decision-making, and behavior of populations in NATO members, partner nations, and neutral nations
Influenced perceptions, decisionmaking, and behavior of populations
Achieved knowledge of adversary networks
Created actionable objectives in adversary networks to facilitate their potential disruption/degradation/destruction (potentially prior to conflict)
Disrupted, degraded, manipulated, and/or destroyed adversary networks
Minimized disruption, degradation, manipulation, and destruction of networks and systems, as well as recovery time and costs, from EW and/or cyberattack
Outcomes
Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts
Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks
Avoided alienation of population, host-nation forces, and host government
Enhanced perceptions of NATO forces (in NATO countries and internationally)
Increased partner cooperation
Set standards for partner nations
Reused captured infrastructure and materiel
Avoided rebuilding costs
Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent
Enhanced NATO-wide public support for policies, objectives, and goals
Achieved desired outcomes through influence on adversary militaries, governments, and populations
Delayed, degraded, disrupted, manipulated, or precluded adversary actions
Reduced effects of adversary attempts to delay, degrade, disrupt, manipulate, or preclude NATO and partner actions
Projected power or demonstrated capabilities using IFCs
Enhanced cyber, EW, IO, and NLW capabilities across all NATO members to deter, cooperate, deploy/sustain, and shape stability and peace
Maintained credibility and legitimacy of NATO and partner forces
Reduced credibility and legitimacy of adversaries
Prevented and deterred malicious cyber and EW activities and increased resilience of critical infrastructure

NOTE: A thick, dark line means a strong, direct, unequivocal connection; a thin, light line means a limited, indirect, or conditional connection. Arrows emanating from a common source have the same color to make them easier for the reader to follow. A blue rectangle indicates an activity with strong links to at least five outcomes.

TABLE A.3

Strength of Connections Between Outputs and Outcomes

	Outcomes																	
Outputs	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Effectively responded to situations despite constraints	2	2	2	1	0	0	0	1	1	1	0	0	2	2	2	2	1	1
Enabled pre-emptive action without appearing to be aggressor	2	0	2	2	1	0	0	1	0	2	2	2	2	1	2	1	0	0
Increased options for engaging targets	2	1	1	1	0	1	1	0	1	1	1	1	0	1	1	1	0	2
Reduced risk of exceeding ROE or Laws of War	2	1	2	2	1	0	0	2	2	2	0	1	0	0	0	0	0	0
Reduced adversary options and imposed costs	2	0	0	0	0	0	0	0	1	1	0	0	1	2	2	0	1	0
Gained time/distance before deciding to take lethal action	2	1	1	1	0	0	0	1	1	1	0	1	0	0	1	0	0	0
Enabled lower-signature clandestine ops	2	2	0	1	0	0	0	0	0	0	0	0	0	1	1	1	0	0
Reduced risk of NATO, partner personnel casualties	1	2	2	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0
Minimized collateral damage and fratricide	1	2	2	2	1	2	2	2	2	2	0	1	1	0	0	0	0	0
Reduced risk to NATO systems or facilities	1	0	0	0	0	0	0	0	1	1	0	0	0	0	2	0	2	2
Gathered intelligence from captured personnel and materiel, as well as from cyber and EW means	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	1
Conserved and augmented lethal capabilities	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Reduced NATO tactical costs (broadly defined)	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Disrupted adversary decision cycle to provide relative advantage to NATO forces and degrade adversary ability to employ forces effectively	2	1	0	0	0	0	0	0	0	1	1	0	2	2	2	2	1	0
Affected perceptions, decisionmaking, and behavior of adversary leadership	2	1	0	0	0	0	0	0	0	2	0	0	2	2	0	1	1	0
Affected perceptions, decisionmaking, and behavior of adversary personnel	2	1	0	0	0	0	0	0	0	1	2	0	2	2	0	1	1	0
Affected adversary leadership's emotional state, judgement, and will to fight	2	1	0	0	0	0	0	0	0	0	2	0	2	2	0	0	1	0
Affected adversary personnel's emotional state, judgement, and will to fight	2	1	0	0	0	0	0	0	0	0	1	0	2	2	0	0	1	0

Table A.3—continued

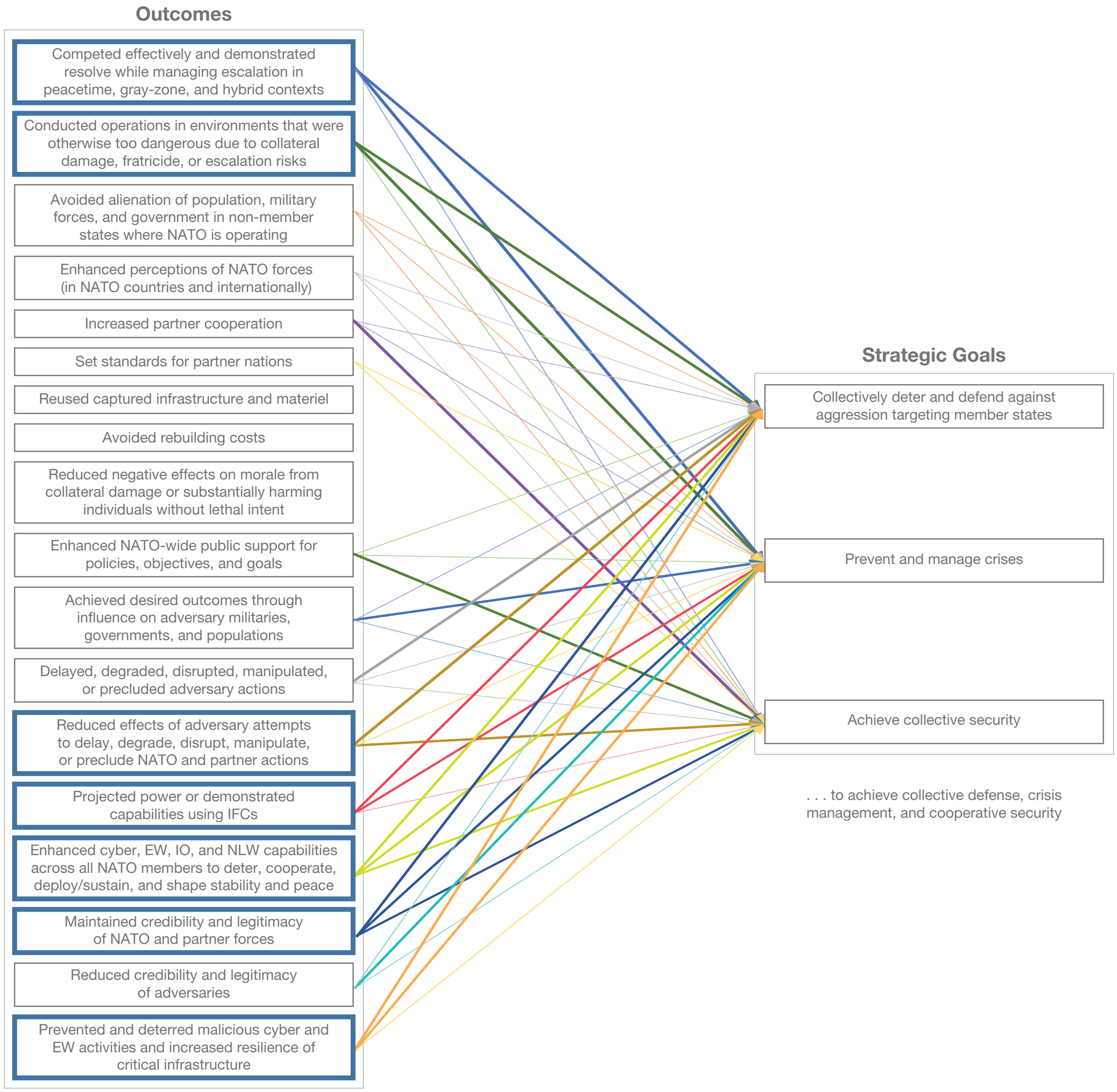
	Outcomes																	
Outputs	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Avoided effects of adversary manipulation of information to affect perceptions, attitudes, decisions, and behaviors of NATO and partner forces	1	0	1	2	2	0	0	0	1	2	0	2	0	1	2	1	0	0
Avoided effects of adversary manipulation of information to affect perceptions, decisionmaking, and behavior of populations in NATO members, partner nations, and neutral nations	1	0	2	2	2	0	0	0	1	2	0	2	0	1	2	1	0	0
Influenced perceptions, decisionmaking, and behavior of populations	1	1	2	2	1	0	0	1	1	2	2	2	2	1	1	1	0	0
Achieved knowledge of adversary networks	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0
Created actionable objectives in adversary networks to facilitate their potential disruption/degradation/destruction (potentially prior to conflict)	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0
Disrupted, degraded, manipulated, and/or destroyed adversary networks	2	2	0	1	0	0	0	0	1	1	1	0	0	2	1	2	1	0
Minimized disruption, degradation, manipulation, and destruction of networks and systems, as well as recovery time and costs, from EW and/or cyberattack	1	0	0	1	1	0	2	1	0	1	1	0	0	1	2	1	2	2

Outcome-to-Strategic Goal Connections

Figure A.3 shows the connections between the outcome and strategic goal levels. Seven outcomes, encased in blue rectangles, were connected to all three strategic goals and have strong connections to at least two of them. Many of the outcomes, though, have at least two strong connections to strategic goals, underscoring the internal cohesion of the logic model overall.

FIGURE A.3

Connections Between the Outcome and Strategic Goal Levels of the NATO-Centric Logic Model


Outcomes
Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts
Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks
Avoided alienation of population, military forces, and government in non-member states where NATO is operating
Enhanced perceptions of NATO forces (in NATO countries and internationally)
Increased partner cooperation
Set standards for partner nations
Reused captured infrastructure and materiel
Avoided rebuilding costs
Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent
Enhanced NATO-wide public support for policies, objectives, and goals
Achieved desired outcomes through influence on adversary militaries, governments, and populations
Delayed, degraded, disrupted, manipulated, or precluded adversary actions
Reduced effects of adversary attempts to delay, degrade, disrupt, manipulate, or preclude NATO and partner actions
Projected power or demonstrated capabilities using IFCs
Enhanced cyber, EW, IO, and NLW capabilities across all NATO members to deter, cooperate, deploy/sustain, and shape stability and peace
Maintained credibility and legitimacy of NATO and partner forces
Reduced credibility and legitimacy of adversaries
Prevented and deterred malicious cyber and EW activities and increased resilience of critical infrastructure
Strategic Goals
Collectively deter and defend against aggression targeting member states
Prevent and manage crises
Achieve collective security
. . . to achieve collective defense, crisis management, and cooperative security

NOTE: A thick, dark line means a strong, direct, unequivocal connection; a thin, light line means a limited, indirect, or conditional connection. Arrows emanating from a common source have the same color to make them easier for the reader to follow. A blue rectangle indicates an activity with strong links to at least two strategic goals.

TABLE A.4

Strength of Connections Between Outcomes and Strategic Goals

	Strategic Goals		
Outcomes	Collectively deter and defend against aggression targeting member states	Prevent and manage crises	Achieve cooperative security
Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts	2	2	1
Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks	2	2	1
Avoided alienation of population, military forces, and government in non-member states where NATO is operating	1	1	1
Enhanced perceptions of NATO forces (in NATO countries and internationally)	1	1	1
Increased partner cooperation	1	1	2
Set standards for partner nations	0	1	1
Reused captured infrastructure and materiel	0	0	0
Avoided rebuilding costs	0	0	0
Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent	0	0	0
Enhanced NATO-wide public support for policies, objectives, and goals	1	1	2
Achieved desired outcomes through influence on adversary militaries, governments, and populations	1	2	1
Delayed, degraded, disrupted, manipulated, or precluded adversary actions	2	1	1

Table A.4—continued

	Strategic Goals		
Outcomes	Collectively deter and defend against aggression targeting member states	Prevent and manage crises	Achieve cooperative security
Reduced effects of adversary attempts to delay, degrade, disrupt, manipulate, or preclude NATO and partner actions	2	1	2
Projected power or demonstrated capabilities using IFCs	2	2	1
Enhanced cyber, EW, IO, and NLW capabilities across all NATO members to deter, cooperate, deploy/sustain, and shape stability and peace	2	2	2
Maintained credibility and legitimacy of NATO and partner forces	2	2	2
Reduced credibility and legitimacy of adversaries	1	2	1
Prevented and deterred malicious cyber and EW activities and increased resilience of critical infrastructure	2	2	1

APPENDIX B

NATO-Centric IFC Metrics

In this appendix, we list the metrics associated with each of the elements of the NATO logic model. We include the metrics for all elements of the NATO logic model, including for the NLW-related elements, because many of these elements also relate to IO, EW, and cyber, and we revised the metrics accordingly. We have also included the results of our evaluation of the metrics. We used the same criteria as the previous study to evaluate metrics on a three-point scale (high, medium, low) in terms of their validity, reliability, feasibility, and timeliness. The criteria for these assessments are summarized in Table B.1; we applied these criteria to evaluate each metric that had been identified, conducting a series of internal workshops in which the values were discussed and debated. The lists of metrics and our evaluations using these criteria are presented in Tables B.2, B.3, and B.4.

TABLE B.1

Criteria for Evaluating Validity, Reliability, Feasibility, and Timeliness of Metrics

	Validity	Reliability	Feasibility	Timeliness[a]
High	Directly measures the element or a close proxy	Well-defined, objective, and stable	Required data sets are readily available and user-friendly	Hours
Medium	Closely related to the element being measured	Some ambiguity, subjectivity, and/or volatility	Required data sets could be collected with limited effort	Days
Low	Indirectly related to the element being measured	Considerable ambiguity, subjectivity, and/or volatility	Required data sets would be challenging to collect	Weeks to years

SOURCE: Savitz, Matthews, and Weilant, 2017.

[a] This refers to the timeliness of receipt of the values of metrics, not timeliness of the effects of IFCs. We selected the values for high, medium, and low timeliness as follows. Values of metrics that are received within hours can inform short-term tactical decisions. Those that are available within days may affect larger operational activities. Those that take weeks or longer can inform future operations.

TABLE B.2

NATO-Centric IFC Activity Metrics

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Hail to clarify, demarcate, and warn	Percentage of targeted population receiving communication	M	M	M	H
	Percentage of encounters in which non-targeted populations receive communication	M	M	M	H
	Percentage of targeted population responding as desired to receipt of communication	H	H	H	H
	Percentage of targeted population responding in undesired ways to communication	H	H	H	H
	Timeline between IFC use and response	M	M	H	H
Reveal other parties' intent	Percentage of targeted population experiencing IFC effects intended to reveal intent	H	M	H	H
	Percentage of encounters in which non-targeted populations are subjected to IFC effects	M	M	H	H
	Percentage of targeted population that responds in ways that reveal intent	H	M	H	H
	Percentage of targeted population that responds in ways that inaccurately suggest hostile intent (false positives)	H	M	H	H
	Percentage of targeted population that responds in ways that inaccurately suggest benign intent (false negatives)	H	M	H	H
	Timeline between IFC use and revelation of intent	M	M	H	H
Deceive, distract, disorient, or confuse	Percentage of targeted population experiencing IFC effects that are deceived, distracted, disoriented, or confused	H	M	M	M
	Percentage of encounters in which non-targeted populations are subjected to IFC effects	M	M	H	H
	Percentage of targeted population that responds in desired ways	H	M	H	H
	Percentage of targeted population that responds in undesired ways	H	M	H	H
	Timeline between IFC use and response	M	M	H	H
Affect mobility: Slow, impede, halt, prevent from approaching or leaving, redirect, disperse, impel departure	Percentage of targeted population experiencing effects that restrict mobility	H	M	H	H
	Percentage of encounters in which non-targeted populations are subjected to IFC effects	M	M	H	H
	Percentage of targeted population that responds in desired ways	H	M	H	H
	Percentage of targeted population that responds in undesired ways	H	M	H	H
	Timeline between IFC use and response	M	M	H	H

Table B.2—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Compel/tactically deter: Convince others to take or not take specific actions	Percentage of targeted population experiencing effects of IFC	M	H	H	H
	Percentage of encounters in which non-targeted populations are subjected to IFC effects	M	M	M	M
	Percentage of targeted population that responds in desired ways	H	H	H	H
	Percentage of targeted population that responds in undesired ways	H	H	H	H
	Timeline between IFC use and response	M	M	H	H
Temporarily incapacitate personnel	Percentage of targeted population incapacitated by IFC	H	H	M	M
	Percentage of encounters in which non-targeted population is incapacitated by IFC	M	H	H	H
	Timeline between IFC use and incapacitation	M	M	H	H
	Duration of incapacitation	M	M	M	M
Incapacitate infrastructure/ materiel	Percentage of targeted infrastructure/materiel incapacitated by IFC	H	H	M	M
	Percentage of encounters in which non-targeted infrastructure or materiel is incapacitated by IFC	M	M	H	H
	Timeline between IFC use and incapacitation	H	M	M	H
Disseminate information to inform and persuade	Percentage of targeted population receiving information	H	M	M	M
	Number of non-targeted people receiving information	M	M	M	M
	Percentage of targeted population informed and/or persuaded in response to receipt of information in accord with intent	H	M	M	L
	Percentage of targeted population that was informed but not persuaded in response to receipt of information in accord with intent	H	M	M	L
	Percentage of targeted population that has a negative response to information (perceptions pushed in opposite direction from intent)	H	M	M	L
	Percentage of targeted population that has a positive response to information (perceptions pushed in the direction of the original intent)	H	M	M	L
	Percentage of targeted population misinterpreting information	H	M	M	L
	Percentage of targeted population correctly/accurately interpreting information	H	M	M	L

Table B.2—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Expose malign information operations	Percentage of targeted population receiving information on (exposure) to malign information operations	H	M	M	M
	Number of non-targeted people receiving information on (exposure) to malign information operations	M	M	M	M
	Percentage of targeted population acknowledging (exposure to) malign information operations as such	H	M	M	L
	Percentage of targeted population that reject/deny/ignore (exposure to) malign information operations as such	H	M	M	L
	Percentage of targeted population that perceive (exposure to) malign information operation	H	M	M	L
	Percentage of targeted population misperceiving exposure as itself a malign information operation	H	M	M	L
	Percentage of targeted population rejecting content of malign information operations based on exposure	H	M	M	L
	Percentage of targeted population accepting content of malign information operations based on exposure	H	M	M	L
	Percentage of targeted population unaffected by exposure of malign information operations	H	M	M	L
	Percentage of targeted population affected by exposure of malign information operations	H	M	M	L
	Percentage of targeted population misinterpreting exposure of malign information operations	H	M	M	L
	Percentage of targeted population correctly/accurately interpreting exposure of malign information operations	H	M	M	L
Disseminate information to affect adversary perceptions and assessments	Percentage of targeted adversary population receiving information	H	M	M	M
	Number of non-targeted people receiving information	M	M	M	M
	Percentage of targeted adversary population affected as intended in response to receipt of information	H	M	L	L
	Percentage of targeted adversary population that was unaffected as intended in response to receipt of information	H	M	L	L
	Percentage of targeted adversary population that has a negative response to information (perceptions pushed in opposite direction from intent)	H	M	L	L
	Percentage of targeted adversary population that has a positive response to information (perceptions pushed in synch with the direction of intent)	H	M	L	L
	Percentage of targeted adversary population misinterpreting information	H	M	L	L
	Percentage of targeted adversary population correctly/accurately interpreting information	H	M	L	L

Table B.2—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Detect and identify sources of EM radiation	Number of EM sources detected	H	H	H	H
	Number of EM sources identified	H	H	H	H
Characterize, locate, and track sources of EM radiation	Percentage of detected/identified EM sources characterized	H	M	M	M
	Percentage of detected/identified EM sources located	H	M	M	M
	Percentage of detected/identified EM sources tracked	H	M	M	M
	Percentage of sources characterized as relevant that are located	H	M	M	M
	Percentage of sources that are characterized as relevant and located that are tracked	H	M	M	M
	Percentage of detected/identified EM sources mistakenly characterized as relevant	H	L	L	L
	Percentage of detected/identified EM sources mistakenly characterized as irrelevant	H	L	L	L
Conduct reconnaissance against, exploit, and establish persistent presence in adversary systems to prepare the cyber battlespace	Percentage of targeted systems exploited	H	H	H	H
	Percentage of targeted systems exploited and established persistence	H	H	H	H
	Number of actionable options created against adversary systems created for future operational use (after persistent presence in network has been established)	H	H	H	H
	Percentage of cyber activity known to have been detected by adversary (as indicated by adversary actions)	M	M	L	L
Degrade, disrupt, and destroy adversary systems and C^4ISR	Number of non-targeted systems affected	L	L	L	L
	Timeline between IFC use and impact	M	M	M	H
	Percentage of targeted adversary systems and C^4ISR degraded, and/or disrupted	H	H	H	H
	Percentage of targeted adversary systems and C^4ISR destroyed	H	H	H	H
	Percentage of targeted adversary systems and C^4ISR exploited	H	H	H	H
	Percentage of attempts to degrade, disrupt, destroy, or exploit adversary systems and C^4ISR that the adversary successfully prevents or mitigates	H	M	H	M

Table B.2—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Defend/protect/ remediate NATO front-line systems against EW	Number of cyberspace defense actions required for NATO front-line systems against EW threats	H	H	H	H
	Number of NATO front-line systems degraded/ disrupted by EW	H	H	H	H
	Number of NATO front-line systems destroyed by EW	H	H	H	H
	Duration of NATO front-line systems being degraded/ disrupted by EW	H	M	H	H
	Number of NATO front-line systems known to have been affected by EW	H	H	H	M
	Duration of known impacts on NATO front-line systems by EW	H	H	H	H
Defend and remediate NATO networks and critical infrastructure (e.g., data backbone) against cyber and EW (includes diagnosis of issues)	Number of cyberspace defense actions required for NATO networks and critical infrastructure by persistent forces against cyberattack	H	H	H	H
	Number of cyberspace defense actions required for NATO networks and critical infrastructure by maneuver forces (Cyber Protection Teams) against cyberattack	H	H	H	H
	Number of NATO networks and pieces of critical infrastructure degraded/disrupted by cyberattack and EW	M	H	H	H
	Number of NATO networks and pieces of critical infrastructure destroyed by cyberattack and EW	H	H	H	H
	Number of NATO networks and pieces of critical infrastructure known to have been exploited by cyber and EW	H	H	H	H
	Duration of NATO networks and pieces of critical infrastructure being degraded/disrupted by cyberattack and EW	M	L	L	L
	Duration of adversary persistent access and exploitation of NATO networks and critical infrastructure by cyber and EW	M	L	L	L
	Timeline to restore full capabilities of network or systems	M	M	M	M
Secure, configure, maintain, and protect existing networks to prevent attacks	Percentage of NATO networks correctly maintained/ configured/secured/protected	H	H	H	H
	Number of outstanding required patches/updates	H	H	H	H
	Number of configuration vulnerabilities exploited by adversary	H	L	L	L
	Percentage of network up time	H	H	H	H

TABLE B.3

NATO-Centric IFC Output Metrics

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Effectively responded to situations despite constraints	Percentage of tactical encounters in which use of IFCs was permissible, but lethal force was not	M	M	H	H
	Whether IFCs are allowed by ROE (binary yes/no distinction)	H	H	H	H
	Degree to which targeted populations perceive IFCs as equivalent to lethal weapons	H	M	M	M
Enabled pre-emptive action without appearing to be aggressor	Percentage of encounters in which pre-emptive action was taken using IFCs, but would not have been with lethal systems due to risk of perception as aggressor	H	M	H	H
	Percentage of encounters in which pre-emptive action was not taken with either IFCs or lethal systems, because would have been perceived as aggressor with either	H	M	H	H
Increased options for engaging targets	Change (absolute or percentage) in number of distinct options available due to use of IFCs	H	M	M	M
	Percentage of encounters in which number of options is increased due to use of IFCs	H	M	M	M
Reduced risk of exceeding ROE or Laws of War	Percentage of encounters in which personnel intentionally use IFCs in ways that exceed ROE or Laws of War	H	L	L	L
	Percentage of encounters in which use of IFCs is proportionate, whereas lethal force would have led to disproportionate/indiscriminate effects	H	L	L	L
	Percentage of encounters in which IFCs enable compliance with ROE/LOW, when lethal force would have resulted in exceeding/violations	H	L	L	L
	Percentage of encounters in which use of IFCs is proportionate, whereas lethal force would have led to disproportionate/indiscriminate effects	H	M	M	M
	Percentage of encounters in which IFCs enable compliance with ROE/LOW, when lethal force would have resulted in exceeding/violations	H	M	H	H
Reduced adversary options and imposed costs	Change (absolute or percentage) in number of distinct options available to an adversary due to use of IFCs	H	L	M	M
	Percentage of encounters in which number of adversary options is reduced due to use of IFCs	H	M	M	M
	Percentage of encounters in which adversary experiences additional costs due to use of IFCs	H	M	M	M

Table B.3—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Gained time/ distance before deciding to take lethal action	Time between initial use of IFCs and when a decision to authorize lethal force would have been required	H	L	M	M
	Percentage of encounters in which lethal action was not taken, but would have been if IFCs were not available to delay decision	L	M	M	M
	Total interaction time between actors for interactions in which IFCs were used compared with those that did not	H	H	M	H
	Commander's perception of increased decision time due to IFCs (Yes/No)	H	M	H	H
	Time required to switch from nonlethal to lethal capability if escalation of force is necessary	M	H	H	H
Enabled lower-signature clandestine ops	Signatures of IFC relative to alternative lethal system	H	H	H	H
	Attributability—probability of being identified as NATO operation with use of IFC, relative to without it	H	M	M	H
Reduced risk of NATO, partner personnel casualties	Percentage of tactical encounters with NATO and/ or partner casualties when IFCs were used relative to those when they were not	H	H	H	H
	Time required to switch from nonlethal to lethal capability if escalation of force is necessary	M	H	H	H
Minimized collateral damage and fratricide	Percentage of tactical encounters in which there were *numerous* injuries among noncombatants	H	M	M	M
	Percentage of tactical encounters in which IFCs were used in which there were any serious/critical/ (life/limb/sensory)/non-buddy care injuries among noncombatants relative to encounters in which IFCs were not used	H	M	H	H
	Percentage of tactical encounters in which IFCs were used in which there were fatalities among noncombatants relative to encounters in which IFCs were not used	H	M	H	H
	Average number of serious injuries among noncombatants per tactical encounter involving IFCs, relative to average number per tactical encounter not involving IFCs	H	M	M	H
	Average number of fatalities among noncombatants per tactical encounter involving IFCs, relative to average number per tactical encounter not involving IFCs	H	M	M	H
	Frequency and magnitude of long-term psychological effects of IFCs by targets	H	L	L	L
	Number of people unintentionally affected by IFC (accuracy/precision of IFC)—per usage	H	M	M	M
	Frequency and severity of long-term biological effects of IFCs on targets	H	L	L	L

Table B.3—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Reduced risk to NATO systems or facilities	Percentage of tactical encounters with system casualties when IFCs were used relative to those when they were not	H	H	H	H
	Time required to switch from nonlethal to lethal capability if escalation of force is necessary	M	H	H	H
	Number of previously unknown cyber and EW vulnerabilities discovered and remediated	H	H	H	H
	Number of successful attacks (kinetic, EW, or cyber) against NATO systems or facilities	H	M	L	L
	Number of critical-infrastructure failures due to attacks	H	M	L	L
Gathered intelligence from captured personnel and materiel, as well as from cyber and EW means	Percentage of encounters in which useful intelligence was gathered from personnel captured through use of IFCs vs. the same metric for lethal weapons	H	M	M	M
	Percentage of encounters in which useful intelligence was gathered from materiel captured through use of IFCs vs. the same metric for lethal weapons	H	M	M	M
	Percentage of network penetrations that resulted in useful intelligence	H	M	M	L
	Number of items of useful intelligence emerging from network penetrations	H	M	M	L
Conserved and augmented lethal capabilities	Percentage of tactical encounters in which lethal capabilities were not used	H	H	H	H
	Percentage of tactical encounters in IFCs increased effectiveness of lethal weapons (e.g., enabled more selective targeting, less restrictive ROE)	H	M	M	H
Reduced NATO tactical costs (broadly defined)	Cost differential between use of IFCs and use of lethal systems (per use, fixed, and life-cycle costs)	H	H	H	H
	Percent reduction in capacity for lethal capabilities due to inclusion of IFCs in vehicles, vessels, backpacks, etc.	H	H	H	H
	Logistics (storage, transportation, resupply, etc.) requirements for IFCs relative to lethal systems	H	H	H	H
	Spare parts and maintenance requirements (time, cost, skill) of IFCs relative to lethal systems	H	H	H	H
	Estimated cost avoidance due to prevention and mitigation of effects of cyber and EW attacks (including downstream impact) relative to cost of prevention and mitigation efforts	H	M	M	M
Disrupted adversary decision cycle to provide relative advantage to NATO forces and degrade adversary ability to employ forces effectively	Timeline of responsiveness of adversary behavior to changing battlespace environment	H	M	M	M
	Number of instances in which adversaries appear to be arraying forces in ways that reflect outdated information	H	L	M	H
	Number of instances when adversary appeared not to make a critical decision within the relevant timeframe	H	L	M	H

Table B.3—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Affected perceptions, decisionmaking, and behavior of adversary leadership	Number of instances in which adversary decisionmaking appears to be influenced by information environment presented by IO campaign	H	L	M	H
	Number of instances in which communications by adversary leaders (both official and personal) reflect information environment presented by IO campaign	H	M	M	H
Affected perceptions, decisionmaking, and behavior of adversary personnel	Number of instances in which adversary small unit and individual decisionmaking appears to be influenced by information environment presented by IO campaign	H	L	M	H
	Number of instances in which communications by adversary personnel (both official and personal) reflect information environment presented by IO campaign	H	M	M	H
	Number of instances in which detained adversary personnel indicate that adversary perceptions, decisionmaking, and behavior reflect information environment presented by IO campaign	H	M	M	H
Affected adversary leadership's emotional state, judgment, and will to fight	Number of instances in which adversary leadership behavior reflects impaired judgement, reduced will to fight, or negative/heightened emotional state during or after IO campaigns, as assessed by intelligence personnel, psychologists, and other subject-matter experts	H	M	M	M
	Number of instances in which statements by adversary leadership reflect inhibited judgement, reduced will to fight, or negative/heightened emotional state, as assessed by intelligence personnel	H	M	M	M
Affected adversary personnel's emotional state, judgment, and will to fight	Number of instances in which adversary small unit or individual behavior reflects impaired judgement, reduced will to fight, or negative/heightened emotional state during or after IO campaigns, as assessed by intelligence personnel, psychologists, and other subject-matter experts	H	L	M	M
	Change in number of desertions before and after/during IO campaign	H	H	L	M
	Change in incidents of subordinates disobeying or failing to carry out orders before and after/during IO campaign	L	H	L	M
	Number of instances in which adversary communications (both official and personal, such as social media posts and email) reflect inhibited judgement, reduced will to fight, or negative/heightened emotional state, as assessed by intelligence personnel, psychologists, and other subject-matter experts	H	M	M	M
	Number of instances in which detained adversary personnel indicate inhibited judgement, reduced will to fight, or negative/heightened emotional state, as assessed by intelligence personnel, psychologists, and other subject-matter experts	H	M	M	M

Table B.3—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Avoided effects of adversary manipulation of information to affect perceptions, attitudes, decisions, and behaviors of NATO and partner forces	Frequency with which public consensus within NATO is broken ("breaking silence")	L	H	H	H
	Percentage of NATO and partner personnel perceiving content of adversary IO campaign as accurate (measured by polls)	H	H	M	L
	Percentage of NATO and partner personnel agreeing with content of adversary IO campaign and considering it important (measured by polls)	H	H	M	L
	Number of NATO and partner personnel resharing content from adversary IO campaign via social media	H	M	M	H
	Leadership retrospective assessment of number of errors they committed due to adversary IO campaigns	H	M	M	L
Avoided effects of adversary manipulation of information to affect perceptions, decisionmaking, and behavior of populations in NATO members, partner nations, and neutral nations	Percentage of population perceiving content of adversary IO campaign as accurate (measured by polls)	H	M	M	L
	Percentage of population agreeing with content of adversary IO campaign and considering it important (measured by polls)	H	M	M	L
	Number of people resharing content from adversary IO campaign via social media	H	M	M	H
	Percentage of population indicating negative perceptions of NATO in ways that reflect adversary IO campaign (measured by polls)	H	M	M	L
	Number and scale of protests against NATO/partner actions or NATO participation in member nations, partners, and neutral nations	M	H	H	H
	Number of media articles reflecting content of adversary IO campaign	H	M	H	H
	Number of lawsuits against individuals or governments that reflect content of adversary IO campaign	H	M	H	H
	Number of political mobilization efforts reflecting agreement with content of adversary IO campaign	H	L	M	M

Table B.3—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Influenced perceptions, decisionmaking, and behavior of populations	Percentage of population perceiving content of IO campaign as accurate (measured by polls)	H	M	M	L
	Percentage of population agreeing with content of IO campaign and considering it important (measured by polls)	H	M	M	L
	Number of people resharing content from IO campaign via social media	H	H	H	H
	Percentage of population indicating negative perceptions of adversary in ways that reflect IO campaign (measured by polls)	H	M	M	L
	Number and scale of protests against adversary actions in adversary nation(s)	M	M	M	M
	Number of media articles reflecting content of IO campaign	H	M	H	H
	Number of lawsuits against individuals or governments that reflect content of IO campaign	H	M	H	H
	Number of political mobilization efforts reflecting agreement with content of IO campaign	H	L	M	M
Achieved knowledge of adversary networks	Percentage of targeted networks exploited	H	H	H	H
	Percentage of targeted networks with established persistence	H	H	H	H
	Duration of persistence in adversary network	H	H	H	H
Created actionable objectives in adversary networks to facilitate their potential disruption/ degradation/ destruction (potentially prior to conflict)	Number of actionable objectives that can result in disruption or degradation of adversary network	H	H	H	H
	Number of actionable objectives that can result in destruction of adversary network	H	H	H	H
Disrupted, degraded, manipulated, and/or destroyed adversary networks	Duration of adversary network disruption/degradation/ manipulation	H	M	M	M
	Extent of adversary network disruption/degradation/ manipulation	H	M	M	M
	Number of targeted systems or networks destroyed	H	H	H	H
Minimized disruption, degradation, manipulation, and destruction of networks and systems, as well as recovery time and costs, from EW and/or cyberattack	Duration of network disruption/degradation/ manipulation	H	H	M	H
	Extent of network disruption/degradation/manipulation	H	H	M	H
	Number of systems or networks destroyed	H	H	H	H
	Reconstitution cost	H	M	H	H

TABLE B.4
NATO-Centric IFC Outcome Metrics

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Competed effectively and demonstrated resolve while managing escalation in peacetime, gray-zone, and hybrid contexts	Percentage of incidents using IFCs that resulted in unwanted escalation divided by percentage of incidents not using IFCs that resulted in unwanted escalation	H	M	H	H
	Percentage of particular peacetime/gray-zone/hybrid incidents in which IFCs were used	M	H	H	H
	Percentage of incidents in which IFCs were used and commanders perceived them as contributing effectively	H	M	H	H
	Degree to which targeted populations perceive IFCs as equivalent to lethal weapons	H	M	M	M
Conducted operations in environments that were otherwise too dangerous due to collateral damage, fratricide, or escalation risks	Frequency of operations within a given timeframe conducted with IFCs available that would not have been conducted without IFCs due to risks of collateral damage, fratricide, or escalation risks	H	M	M	H
Avoided alienation of population, military forces, and government in non-member states where NATO is operating	Non-member nation public opinion of use of IFCs, measured by polls	H	M	L	L
	Non-member nation public opinion of NATO force presence and actions, measured by polls	L	M	L	L
	Frequency and scale of protests and riots against NATO presence, actions	L	H	H	H
	Frequency and scale of protests and riots related to events involving NATO use of IFCs	M	M	H	H
	Frequency and scale of protests and riots against NATO use of IFCs	H	M	H	H
	Degree of military cooperation/permissiveness (high, medium, low), as assessed by personnel from NATO nations	L	M	H	M
	Non-member nation forces' perception of NATO use of IFCs, as assessed by personnel from NATO nations who are engaged with them	H	M	M	M
	Non-member nation government's perception of NATO use of IFCs, as assessed by personnel from NATO nations who are engaged with them	H	M	M	M
	Frequency of negative public statements by government figures about NATO use of IFCs	M	H	H	H
	Degree to which targeted populations perceive IFCs as equivalent to lethal weapons	H	M	M	M

Table B.4—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Enhanced perceptions of NATO forces (in NATO countries and internationally)	Degree to which international public opinion perceives IFCs as equivalent to lethal weapons, measured by polls	H	M	L	L
	Degree to which NATO member states' public opinion perceives IFCs as equivalent to lethal weapons, measured by polls	H	M	L	L
	International public opinion of NATO use of IFCs, measured by polls	H	M	L	L
	International public opinion of NATO force presence and actions in a third country, measured by polls	L	M	L	L
	Frequency and scale of protests and riots internationally against NATO presence, actions in third country	L	H	H	H
	NATO member states' public opinion of NATO use of IFCs outside NATO territory, measured by polls	H	M	L	L
	NATO member states' public opinion of NATO military use of IFCs within NATO nations or along their borders, measured by polls	H	M	L	L
	Frequency and scale of protests and riots in NATO nations against NATO presence, actions in another country	L	H	H	H
	Frequency and scale of protests and riots related to events involving NATO use of IFCs within NATO territory or along NATO borders	M	M	H	H
	Frequency and scale of protests and riots within NATO nations related to IFC use within the NATO nations or along their borders	H	M	H	H
	NATO nations' public opinion regarding NATO force presence and actions in another country, measured by polls	L	M	L	L
Increased partner cooperation	Degree of military cooperation/permissiveness (high, medium, low), as assessed by personnel from NATO nations	L	M	H	M
	Number of joint exercises, patrols, or other activities between NATO and partner nation forces	L	M	H	H
Reused captured infrastructure and materiel	Timeline to repair after IFC usage relative to timeline imposed if needed to replace or use alternative	H	M	M	M
	Resource requirements to repair after IFC usage relative to resources required to replace or use alternative	H	M	M	M
Avoided rebuilding costs	Timeline to repair after IFC usage relative to timeline imposed if needed to replace or use alternative	H	M	M	M
	Resource requirements to repair after IFC usage relative to resources required to replace or use alternative	H	M	M	M

Table B.4—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Set standards for partner nations	Number of partner nations adopting IFCs and related tactics	H	H	H	H
	Number of partner nations violating Laws of War	L	M	M	M
	Number of partner nations found to have used IFCs for human-rights violations	H	L	L	L
Reduced negative effects on morale from collateral damage or substantially harming individuals without lethal intent	Percentage of surveyed personnel who feel that IFCs reduce collateral damage	M	M	L	L
	Percentage of surveyed personnel who indicate that collateral damage contributed to negative morale	M	M	L	L
	Percentage of surveyed personnel who feel that they used lethal force in an unethical way	M	M	L	L
	Frequency of posttraumatic stress disorder	L	L	L	L
	Frequency of suicide attempts	L	L	L	L
Maintained credibility and legitimacy of NATO and partner forces	Percentages of NATO and partner nation populations that view NATO and partner activities as legitimate, as measured by polls	H	M	M	L
	Percentage of adversary population that views NATO and partner activities as legitimate, as measured by polls	H	L	L	L
	Percentage of NATO and partner nation populations that views NATO and partners as credible actors, as measured by polls	H	M	M	L
	Percentage of adversary population that views NATO and partners as credible actors, as measured by polls	H	L	L	L
	Number of favorable UN resolutions regarding NATO actions	H	H	H	H
	Number of unfavorable UN resolutions regarding NATO actions	H	H	H	H
Reduced credibility and legitimacy of adversaries	Percentage of NATO and partner nation populations that views adversary activities as legitimate, as measured by polls	H	M	M	L
	Percentage of adversary population that views adversary activities as legitimate, as measured by polls	H	L	L	L
	Percentage of NATO and partner nation populations that views adversary as a credible actor, as measured by polls	H	M	M	L
	Percentage of adversary population that views adversary as a credible actor, as measured by polls	H	L	L	L
	Number of favorable UN resolutions regarding adversary actions	H	H	H	H
	Number of unfavorable UN resolutions regarding adversary actions	H	H	H	H

Table B.4—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Enhanced NATO-wide public support for policies, objectives, and goals	Percentages of NATO member states' populations supporting NATO policies, objectives, and goals, as measured by polls	H	M	M	L
	Variation in percentage of NATO member population that supports NATO policies, objectives, and goals across NATO members, as measured by polls	H	M	M	L
	Number of public incidents (e.g., protests) within NATO states that indicate opposition to NATO policies, objectives, or goals	H	M	H	H
	Percentage of population in NATO member states that supports maintaining or increasing levels of funding, as measured by polls	M	M	M	L
	Percentage of population in NATO member states that supports NATO membership, as measured by polls	M	M	M	L
Achieved desired outcomes through influence on adversary militaries, governments, and populations	Number of incidents in which an attempt to influence adversary governments and populations resulted in the desired outcome	H	M	M	M
	Number of incidents in which an attempt to influence adversary governments and populations resulted in an undesired outcome	H	M	M	M
Delayed, degraded, disrupted, manipulated, or precluded adversary actions	Number of targeted adversary actions delayed, disrupted, degraded, manipulated, or precluded by use of IFCs	H	M	M	M
	Number of actions affected outside of targeted adversary population (e.g., we tried to affect red but affected green)	M	M	M	M
	Costs imposed on adversary (e.g., platform or infrastructure losses, financial costs, delays)	H	M	M	M
Reduced effects of adversary attempts to delay, degrade, disrupt, manipulate, or preclude NATO and partner actions	Number of NATO and partner actions delayed, disrupted, degraded, manipulated, or precluded due to adversary actions	H	M	H	H
	Extent of delay, disruption, degradation, manipulation, or denial of NATO and partner actions due to adversary actions	H	M	H	H
	Costs imposed on NATO and partners (e.g., platform or infrastructure losses, financial costs, delays)	H	M	H	H
	Costs incurred due to system and network degradation/disruption/denial/manipulation/destruction	H	M	H	H
	Number of operations delayed incurred due to system and network degradation/disruption/denial/manipulation/destruction	H	M	H	H

Table B.4—continued

Element of Logic Model	Metric	Validity	Reliability	Feasibility	Timeliness
Projected power or demonstrated capabilities using IFCs	Number of operations beyond NATO members' territory supported by IFCs	H	H	H	H
	Number of instances of ground/air/sea/space conflict avoided through the use of IFCs as part of power projection or demonstration of capabilities	H	L	M	M
	Number of adversary actions that were deterred through the use of IFCs	H	L	M	M
	Number of public or deliberately attributable demonstrations of IFCs	H	H	H	H
Prevented and deterred malicious cyber and EW activities and increased resilience of critical infrastructure	Network downtime due to known or suspected hostile cyber or EM activity	H	H	H	H
	Number of disruptions due to known or suspected hostile cyber or EM activity	H	H	H	H
	Number of cyber or EM actions that were deterred	H	L	M	M
	Number of instances in which NATO is targeted by known or suspected hostile cyber or EM activity	M	M	M	M
Enhanced cyber, EW, IO, and NLW capabilities across all NATO members to deter, cooperate, deploy/sustain, and shape stability and peace	Number of new policies/processes created and/or existing policies/processes updated by NATO and/or member states to improve future security	H	H	H	H
	Extent of documentation of NATO standards for IFCs	H	H	H	H
	Number of members meeting NATO target capabilities for IFCs	H	M	H	H
	Frequency of updates of NATO standards and capabilities for rapidly evolving IFCs (especially cyber and EW)	H	H	H	H

APPENDIX C

NATO-Centric IFC Vignettes

As was mentioned in Chapter Three, we developed a set of 11 vignettes that involved NATO use of NLWs, IO, EW, and cyber capabilities in a wide range of situations. Having briefly summarized them in Chapter Three (in Table 3.5, recapitulated below as Table C.1), we provide more details on each of them in this appendix, in the order presented in the table.

Don't Beam Me Up

Context. The tiny East African country of Lilliput hosts military bases from multiple NATO members. However, it also hosts a military base from the more distant nation of Scarlett, which has a tense relationship with several of those members. A number of personnel from NATO nations in Lilliput have experienced

TABLE C.1

Vignettes for the NATO-Centric Logic Model

Vignette	Description
Don't Beam Me Up	In a small nation that hosts bases from many other powers, forces from one of those powers are targeting NATO forces using microwave beams, aiming blinding lasers at aircraft and ships, and using EW to crash UAVs.
Order on the Border	NATO forces on the border between a NATO member and hostile nation are trying to get migrants not to cross in unauthorized locations.
Hazy Shade of Winter	A ransomware cyberattack has shut down NATO nations' facilities for handling liquefied natural gas imports.
Gently Seizing Control of the Very Dangerous Weapons	NATO forces are attempting to use multiple IFCs to seize a facility for manufacturing and storing chemical and biological weapons, while trying to minimize the risk of releases and aiming to capture systems, personnel, and computer systems intact.
Tanks, but No Tanks	NATO forces are using various IFCs to impede the advance of tanks from a hostile nation into a partner nation.
A Friend in Need or a Foe Indeed	Boats departing from a war-torn nation are approaching a NATO warship, but it is unclear whether the boat contains migrants or potential terrorists who may want to launch a suicide attack.
Perplexing Perimeter Protection Problems	Deployed NATO forces are considering use of various IFCs to deter locals from stealing fencing and security equipment from base perimeters.
Northern Exposure	NATO forces are trying to help a NATO member restore order in an Arctic territory over which it has sovereignty, despite protests instigated by a hostile nation.
Balkan Blues	NATO forces are using multiple IFCs to try to prevent fighting between two groups in the Balkans.
Nightmare at the Museum	NATO forces are trying to counter an attempt by personnel in unmarked uniforms from Vermilion to infiltrate and take over NATO member Fractus.
Not Quiet on the Eastern Front	A nation adjoining several NATO members has launched a full-scale invasion of their territories, and Article V has been invoked. In the heat of large-scale combat, NATO forces are using IFCs to complement more traditional weapons.

"Havana Syndrome" (potentially permanent brain injuries caused by beams of microwave radiation, also termed "immaculate concussions"). Intelligence indicates that these injuries resulted from attacks by Scarlett. In addition, blinding lasers have been aimed at NATO ships and aircraft from the Scarlett base, injuring personnel. Moreover, NATO uncrewed aerial vehicles (UAVs) have been manipulated and deliberately crashed, apparently as the result of Scarlett EW. Scarlett denies any possible responsibility for any of these events, and argues that they are not actually happening, despite assiduous collection of evidence by various NATO nations.

Note that this scenario is based on real-world precedents: U.S. embassy personnel have been subjected to microwave attacks, U.S. military pilots in other countries have been targeted with blinding lasers, and Iran electronically diverted and seized a U.S. UAV in 2011.

NATO posture and capabilities. NATO forces have not yet taken any action against Scarlett, in an effort to prevent escalation. They do, however, have an array of IFCs that could be used to push back without using lethal force.

- NATO forces have multiple NLWs available:
  - acoustic hailers to hail and warn other parties
  - eye-safe laser dazzlers to create glare without causing permanent injury
  - the ADS, a millimeter-wave emitter that creates a temporary heating sensation but no permanent effects
  - Radio Frequency Vehicle Stoppers (RFVSs) to shut down a vehicle's electronics
  - the Vessel Incapacitating Power Effect Radiation (VIPER) system to shut down a vessel's electronics
  - Maritime Vessel Occlusion Technologies (MVSOTs) to entangle propellers.
- NATO forces have initiated an IO campaign to inform the local community of the dangers posed by the use of blinding lasers to both military and civilian air traffic.
- NATO forces can use EW capabilities to further track the sources of "immaculate concussion" attacks, as well as both EW and cyber capabilities to disrupt Scarlett operations, but with a risk of escalation.

Adversary capabilities. In addition to various lethal capabilities on its base, vehicles, aircraft, and vessels, Scarlett is assumed to have a range of NLW, IO, EW, and cyber capabilities.

Order on the Border

Context. Filder, which has a hostile relationship with NATO and the EU, has been creating issues by transporting thousands of migrants from other parts of the world to remote locations along the border with NATO member Glorin. Filder has conducted an IO campaign promising these migrants that as soon as they cross the border into Glorin, they will be free to live almost anywhere in Europe that they choose. However, Glorin insists on orderly entry and asylum procedures. Filder police continually goad the migrants to try to cross the border. There are no housing facilities for the migrants, whose condition quickly deteriorates due to a lack of food, shelter, and medical care. The migrants are angrily shouting at Glorin's border guards, demanding that gates be opened through the hard-to-climb fence, which the Glorin border guards will only do if the migrants form orderly lines and avoid stampeding. Meanwhile, behind the migrants, Filder police are physically pushing the migrants into the border fence (hitting some of them with truncheons), injuring some of the migrants, and threatening to shoot any who try to move away from the border. Filder has an extensive IO campaign for global media in which it places all blame on Glorin for keeping the migrants out.

After a day or so, Glorin has set up a temporary land port of entry at a nearby location, which will be open to asylum-seekers. However, Glorin continues to insist that entry be managed, and seeks to prevent crossings elsewhere. NATO forces have been deployed to assist with this operation, and they want to avoid injuries (including from direct use of force, migrant stampedes, and the elements) while ensuring both that Glorin retains control of its borders and that it accepts claims for asylum. Meanwhile, some of the migrants are trying to cut through or scale the border fence, and some have formed a dangerously large, tight crowd at the port of entry.

This scenario has a real-world precedent. In 2021, Belarus invited people to fly in from Iraq so that they could enter the European Union; Belarus then moved those people to its border with Poland and forced them to remain there, demanding that Poland permit them to enter.

NATO posture and capabilities. Part of NATO's focus is on conducting an IO campaign to explain entry requirements (i.e., right to asylum, if warranted) and the entry process to the migrants, as well as their rights within Filder. Some of this IO campaign is conducted electronically by sending alerts to migrants' phones in their languages, but it is also done through large signs and acoustic hailers. The acoustic hailers could be used to warn migrants not to cross in unauthorized locations, and to tell them to form an orderly line at the land port of entry, as well as to avoid stampedes that could injure them.

To the extent that migrants continue to try to cross in a dangerous manner or in unauthorized locations, they can be dissuaded through the use of a couple of NLWs. Laser dazzlers can create glare, and the ADS can create a heating sensation that encourages people to back off. Pepper balls that emit pepper spray on a large scale, or tear-gas canisters, could also be used sparingly.

Adversary capabilities. Filder's efforts are driven by an IO campaign. Filder is not currently using lethal weapons, though its personnel are threatening migrants with guns. The only NLWs it is capable of employing at the moment are truncheons, and it is not utilizing any cyber or EW capabilities.

Hazy Shade of Winter

Context. Facilities across Europe for handling incoming shipments of liquefied natural gas (LNG) have been shut down by ransomware cyberattacks just before winter, as demand for gas is rising. Intelligence suggests that the attacks are coming from state-backed hackers in Vermilion, which exports gas to Europe via pipeline, but Vermilion denies responsibility. Its culpability appears to be confirmed by additional actions: It has implemented an IO campaign through social media influencing citizens of affected nations to pressure their governments to pay ransom, and to riot in the streets if the government does not comply.

This vignette is loosely based on a real-world ransomware attack against an oil pipeline in 2011, in which the perpetrators were suspected to have been hackers linked to the Russian government.

NATO posture and capabilities. To address the situation, NATO forces will take several complementary approaches. First, they will create an IO campaign to publicize NATO efforts to return LNG facilities to full functionality, and to restore public confidence in NATO and in the governments of alliance members. Second, NATO is responding by utilizing the Cyber Space Operations Center to deploy rapid-reaction cyber defense teams in support of affected allies. These cyber teams will identify the parties who were responsible based on cyber forensics, as an aid in reinforcing norms of responsible behavior in cyberspace. Finally, NATO teams could use cyber capabilities to establish persistence in Vermilion's networks, facilitating tracking of responsible parties and enabling future action.

Adversary capabilities. The other side is advanced and actively engaged in cyber and IO, but it is not able to use EW or NLW capabilities in this context.

Gently Seizing Control of the Very Dangerous Weapons

Context. Laputa, a large nation on the southern shores of the Mediterranean, has collapsed into a multisided civil war. A radical group, Al-Jabr, has taken over a large fraction of its territory. NATO forces are intervening on a limited scale, primarily from offshore, to try to contain and manage the conflict; NATO does not have ambitions of resolving the conflict.

Al-Jabr has established a chemical and biological weapon complex along the coast, with facilities that are suspected to be manufacturing and storing both mustard agent and an unidentified contagious disease. NATO nations' intelligence indicates that these weapons will likely be used for terrorist attacks in Europe, including against NATO members.

This vignette draws on anticipated problems with trying to counter chemical weapon facilities in Syria after the Assad regime used chemical weapons against its population, though such situations were avoided when the regime, under duress, formally handed over much of its chemical arsenal. Similar issues have occurred during fighting near nuclear facilities in Ukraine in 2022.

NATO posture and capabilities. NATO forces aim to prevent employment of existing weapons, to prevent future production of them, and to acquire as much knowledge as possible of Al-Jabr's programs to date. They will accomplish this by seizing control of the complex just after dusk on a Thursday. They want to be able to conduct extensive intelligence collection regarding the state of the complex, to secure destruction of stockpiles and machinery where possible, to collect small and safe-to-carry items for further analysis, and to detain key personnel for questioning.

A key challenge is that NATO forces want to do all of this while minimizing the risk of accidental releases or exposure (e.g., from shards or bullets piercing containment). Also, NLWs may be used to help capture personnel, rather than killing them. NATO forces will use the following capabilities:

- cyber and EW tactics to disable and affect specific systems
- RFVSs to incapacitate patrolling vehicles
- laser dazzlers to create glare that hinders the other side's ability to shoot accurately
- flash-bang grenades to incapacitate personnel in confined spaces
- bean bags and grenades dispersing rubber pellets to inflict limited injuries
- Pre-Emplaced Vehicle Stoppers (PEVSs) to impede attempts to flee by car
- a complete IO plan to address the risk of potential releases being used by the other side for claims that NATO introduced chemical or biological weapons, as well as to counter claims that this is a prelude to NATO attempting to occupy large parts of Laputa.

Adversary capabilities. Al-Jabr forces have no cyber, EW, or NLW capability, but are good at IO. They have been effective at manipulating social media, particularly inspiring fear among middle and high school students who find Al-Jabr especially menacing.

Tanks, but No Tanks

Context. Vermilion, a large nation that is hostile to NATO, has massed tanks on the border of Emerald, a NATO partner for peace. Vermilion is also backing separatist forces in Emerald's province of Sanguis, and has supported a few leaders in Sanguis who have declared an independent republic. Vermilion has begun an IO campaign to promote both its invasion and the independence of Sanguis.

This vignette is loosely based on the situation in Ukraine in late 2021 and early 2022, before the all-out Russian invasion of that country.

NATO posture and capabilities. NATO is deploying its own peacekeeping force to the region to pressure Vermilion not to invade Emerald, and has started an IO campaign to show that Vermilion is the aggressor. NATO commanders are concerned that if personnel from NATO members use lethal force—even a single shot in the wrong context—that could lead to disaster for Emerald and Sanguis, as well as escalation between NATO and Vermilion. To slow and/or stop the advance of Vermilion's tanks without causing escalation or even a full-scale war, NATO forces will use the following capabilities:

- cyber and EW tactics to disable and affect specific systems
- laser dazzlers to create glare that hinders personnel from Vermilion or Sanguis from targeting effectively or even operating equipment
- RFVSs to incapacitate advancing vehicles supporting the armored divisions
- the Single Net Solution-Remote Deployment Device (SNS-RDD) to stop Vermilion armor by entangling the tracks
- having Emerald's forces clandestinely put in PEVSs to incapacitate vehicles
- if absolutely necessary, destroying infrastructure (bridges) along the path of Vermilion forces to halt their advance.

Adversary capabilities. Vermilion has a wide array of cyber, EW, IO, and NLW capabilities. NATO forces have some ability to resist cyber and EW attacks, but Emerald networks are highly vulnerable to them. Vermilion also has an ADS that it uses to create a heating sensation, particularly when it wants to capture people, rather than killing them. Its use of laser dazzlers interferes with NATO and Emerald forces' ability to target accurately, or even to operate equipment. It also focuses heavily on its IO campaign, claiming that it is on a rescue mission to protect Sanguis from Emerald.

A Friend in Need or a Foe Indeed

Context. The eastern Mediterranean nation of Cerulean has become engulfed in a civil war. Migrants fleeing Cerulean have become increasingly desperate to reach Europe, with record numbers of people trying to cross in overloaded boats. There are now dozens of refugee boats crossing the Mediterranean at any given moment, creating a humanitarian disaster. At the same time, intelligence indicates that religious extremist groups in Cerulean are smuggling their followers into Europe disguised as refugees, in order to then launch terrorist attacks. A series of terrorist attacks across Europe on a single evening underscores the threat; some of the attacks appear to have involved suicide bombers, and intelligence suggests that Cerulean extremists were behind them. This threat has been reinforced by recent Cerulean IO campaigns, which have called for the total destruction of people in Europe who do not share their beliefs.

This vignette echoes both the large-scale migrant movements and occasional terrorist attacks of the 2010s.

NATO posture and capabilities. NATO warships have been sent into the region to assist with command and control of smaller law-enforcement vessels in the area, to locate migrant vessels, and to conduct search and rescue operations as required. After locating a small group of dhows overloaded with people, a NATO warship maintains a 2-km (1.2-mile) range while deploying small boats to approach the dhows more closely. Two dhows refuse to stop and try to approach the NATO warship. It is not clear what the dhows' intentions are. It is possible that they contain refugees seeking assistance, but also possible that they contain terrorists who are attempting a suicide attack, similar to the explosive-boat attack on the USS *Cole* in 2000.

To minimize the risk of harming migrants but to maintain the required security zone around the warship, NATO forces could use the following NLW capabilities:

- acoustic hailing devices to warn the dhows that they need to back away from the warship
- laser dazzlers to hinder the dhows' pilots from maneuvering effectively and underscore the warnings
- ADS to hinder the other side from approaching by creating a heating sensation
- VIPER to stop the engines of the approaching dhows
- MVSOTs to foul the propellers of the dhows.

Adversary capabilities. The other side has no cyber, EW, or NLW capability, but it is good at IO. If NATO uses lethal force or appears to be causing drownings, extremist propaganda will take advantage of it.

Perplexing Perimeter Protection Problems

Context. After massive terrorist attacks in Europe by groups based in the African nation of Magenta, NATO gets involved in operations to pursue extremists there. However, newly established NATO bases in Magenta have a recurring perimeter-security problem. Children and young adults in impoverished Magenta regularly approach the perimeter to steal fencing materials, floodlights, mounted cameras, and other items along the perimeter. These activities reduce security in two respects: Not only do they degrade security infrastructure, but they also create "noise"—constant human activity that is illicit, but not threatening—that actual attackers can use for concealment.

This vignette is based on issues that arose in Afghanistan, where theft of materials from base perimeters was a persistent problem.

NATO posture and capabilities. NATO seeks to drive away these children and young adults without harming them. It does so through a combination of

- IO campaigns to warn of the risks
- acoustic hailing devices to warn people to get away
- eye-safe laser dazzlers to indicate that they are being watched and disorient them
- brief usage of the ADS to create a heating sensation to cause them to flee.

Adversary capabilities. The disorganized thieves have no NLW, IO, EW, or cyber capabilities.

Northern Exposure

Context. State-owned enterprises from the nation of Scarlett are investing heavily in Septentrio, an Arctic territory under the sovereignty of Regnum, a NATO nation. Regnum subsidizes Septentrio and provides for its security, though there is also an independence movement. Scarlett has started an IO campaign urging Septentrio residents to declare independence, and is manipulating various mainstream and social media channels to foster this sentiment.

When a warship from Regnum patrolling Septentrio's waters attempts to enter its main port for refueling, it finds that fishing vessels have blocked the entrance the port. Some of them seem to be taunting the warship, approaching it and going in circles around it as it sits offshore. There are also land-side protesters who demand that the ship, if it docks, be impounded and transformed into the flagship of a new navy for Septentrio.

Efforts by authorities to clear the protesters and to keep small, open boats from approaching the warship have not gone well. A video of land-side protesters being hit with water cannons, and two boaters being knocked into the water by them, has been watched millions of times around the world. While the boaters were rescued, and are now being treated for hypothermia in a local hospital, the Scarlett IO campaign has used these images to further increase the outrage of the local population.

This vignette does not have a historical precedent, but there are concerns about how potential Chinese investment in Greenland and Greenland's independence movement could lead to various types of tensions among Greenland, Denmark, and China.

NATO posture and capabilities. At Regnum's request, NATO nations are sending ships and personnel to help restore order in its territory. To minimize the risk of harming people, but to maintain the required security zone around warships and disperse the land-side protesters, NATO forces will use the following capabilities:

- acoustic hailing devices to warn the protestors that they need to depart the area
- laser dazzlers to hinder the other side from maneuvering effectively
- ADS against personnel on open boats, on decks, and on land
- MVSOTs to foul ship propellers and VIPER to disable their engines, enabling the ships to be moved around by tugboats.

Adversary capabilities. Scarlett has no local EW or NLW capability, but it is good at IO and may use cyberattacks to disrupt NATO efforts.

Balkan Blues

Context. NATO has been continually aiming to stabilize select countries in the Balkans after a series of wars during the 1990s. The government of one of those nations, Indignan, declares that all vehicles entering their country must display special decals with the symbols and motto of Indignan. In response, along the border between Iratus and Indignan, a large number of non-uniformed individuals from Iratus have blockaded the border crossing with large trucks. It is unclear whether these individuals are civilians or military personnel. Moreover, a municipal building in Indignan where the decals were issued was destroyed in a fire. While there is evidence of arson, authorities have been unable to determine who was responsible, and there has been speculation that the attack was by agents from Iratus.

Public opinion has been inflamed in both Iratus and Indignan. After effective radio and internet campaigns on both sides of the border to attack the other side, large numbers of people from both Iratus and Indignan have made their way to the small border town. Many appear to be peaceful, but a small contingent on each side seems eager for a fight.

This vignette is meant to echo tensions that have arisen in Serbia, Kosovo, and elsewhere in the Balkans, including disputes regarding the use of one country's license plates in another's territory.

NATO posture and capabilities. NATO patrols have been moved to the area to prevent escalation between people from Iratus and Indignan, and if at all possible, to keep them apart. The NATO forces have copious NLWs available for crowd control. These include acoustic hailers to communicate and warn, laser dazzlers to disorient and discomfit, blunt-impact munitions, tasers, riot-control agents, the ADS to create a heating sensation, and three devices to stop vehicles from plowing into pedestrians: RFVSs, PEVSs, and the SNS-RDD. NATO is also conducting an IO campaign to encourage people to remain peaceful and to return to their homes.

Adversary capabilities. Forces from both Iratus and Indignan have strong IO capabilities, as well as limited NLW, EW, and cyber capabilities. Iratus continues to ramp up tensions with an IO campaign that is supported and magnified by Vermilion, a large nation that has historically been hostile to NATO.

Nightmare at the Museum

Context. Vermilion, a large nation hostile to NATO, is attempting to destabilize the NATO nation of Fractus, which has a large minority of Vermilion-speakers. Vermilion has initiated an IO campaign targeting Vermilion-speakers in Fractus, calling on them to stand up for their rights. A Fractus museum has recently installed a new art exhibition that celebrates Fractus heritage while completely ignoring the cultural contributions of Vermilion-speakers in Fractus. A relatively small protest outside the museum escalated when one protester was physically restrained from entering the museum, and subsequently arrested. Over the next several days, thousands of protesters, including some coming from Vermilion, gathered around the museum. Many of them are openly wearing body armor and unmarked uniforms, and some have brought guitar cases that they subsequently opened to reveal guns. Fractus police forces were quickly overwhelmed as the protesters began to riot, so the Fractus police were pushed out of the vicinity of the museum and forced to retreat several blocks away. Additional armed personnel in unmarked uniforms and body armor have blocked access to the city government center and seized television and radio stations. Overall, these forces appear to be well-disciplined, and their movements are highly coordinated.

This vignette reflects tensions that occurred in Estonia in 2007, when Russian propaganda regarding Estonian plans to move a Soviet-era monument inspired riots by ethnic Russians within Estonia.

NATO posture and capabilities. At the request of the Fractus government, a company of NATO soldiers from the Enhanced Forward Presence battlegroup is moving towards the city. The NATO forces have all NLWs available for use: acoustic hailers to communicate and warn, laser dazzlers to create glare, blunt-impact munitions, tasers, riot-control agents, ADS to create a burning sensation, and RFVSs, SNS-RDD, and PEVSs to disable vehicles. NATO has initiated an IO campaign asserting that the uniformed personnel are Vermilion soldiers who have infiltrated into Fractus.

Adversary capabilities. Vermilion uses an IO campaign to initially deny that it has any soldiers in Fractus, followed by an IO campaign stating that a "security operation" became necessary to protect Vermilion-speakers and to prevent rioting people in Fractus from crossing the border into Vermilion.

Not Quiet on the Eastern Front

Context. The large, hostile nation of Vermilion has launched an invasion of several NATO members, causing NATO to invoke Article V (an attack on one nation is an attack on all). NATO forces dominate the skies and have good air and missile defenses on the ground, but Vermilion's massive number of ground forces are pushing back much smaller numbers of NATO defenders.

This vignette does not have a precedent, but is based on concerns that Russia could invade some of its neighbors who belong to NATO.

NATO posture and capabilities. This is mostly a fight involving lethal weapons. However, IFCs can play important complementary roles. Cyber and EW capabilities can help to disable Vermilion forces, while also protecting against Vermilion attacks in the same domains. IO also plays an important role in ensuring international support for the coalition, including in some NATO members. NLWs also have some utility; for example, RFVSs cause Vermilion vehicles to inexplicably shut down, frustrating their occupants and preventing forward movement. Mostly, though, NLWs are highly disruptive to Vermilion's war plans because Vermilion personnel are psychologically unprepared for their effects. Vermilion fighters who have been trained to brave bullets and bombs find themselves discomfited by bursts of glare from eye-safe laser dazzlers mounted on uncrewed aircraft. Similarly, intermittent NATO use of the ADS to create a heating sensation causes whole units to break and run, despite the fact that they previously held together under artillery bombardment.

Adversary capabilities. Vermilion forces have a panoply of cyber, EW, and IO capabilities. However, they are dismissive of NLW systems, given that this is a lethal fight.

APPENDIX D

Brief Overview of Non-Lethal Weapons

In our previous report (Romita Grocholski et al., 2022), we developed a nondoctrinal definition of NLWs, drawing on a definition from DoD Directive 3000.03E:

> Systems and capabilities that can be used in all phases of conflict to stop, deter, deny, delay, or temporarily incapacitate targeted personnel and materiel by producing predictable, immediate effects that are intended to be reversible and minimize unnecessary destruction and loss of life. (Romita Grocholski et al., 2022, p. 3)

NLWs fall naturally into a series of broad categories, depending on the types of effects they produce. As noted in the prior report, which provides more detail, these categories include the following:

- **Acoustic systems**, such as the acoustic hailing device, to communicate, warn, or create irritating sounds, or the experimental concept of Laser-Induced Plasma Effects (LIPE), using lasers to create a sound-emitting plasma at a distance.
- **Laser dazzlers**, such as the Ocular Interrupter (OI) and Long-Range Ocular Interrupter (LROI), which create glare that has no permanent effects on vision, but impair people and effectively warn them to back away.
- **Integrated-effects systems**, such as the Escalation of Force (EoF) Common Remotely Operated Weapons Station (CROWS), which is currently being prototyped; it uses acoustic systems, laser dazzlers, and other lights in concert.
- **Flash-bang grenades**, which create light and sound that distract and temporarily incapacitate.
- **Blunt-impact munitions**, such as beanbag rounds and rubber bullets, that strike people but are meant to have limited effects compared with intentionally lethal weapons; the effects are often temporary.
- **Electro-muscular incapacitation systems**, such as Tasers, which use an electrical current to incapacitate at short ranges.
- **Riot-control agents**, such as pepper spray and tear gas. Note that these are not permitted in combat, under the Chemical Weapons Convention, but can be used in noncombat situations.
- **Millimeter-wave systems**, such as the Active Denial System (ADS), which emit focused beams to create a temporary heating sensation to discomfit personnel.
- **Microwave systems** that can incapacitate vehicles or vessels, such as the Radio Frequency Vehicle Stopper (RFVS) or the Vessel Incapacitating Power Effect Radiation (VIPER) system.
- **Mechanical vehicle/vessel-stopping technologies**, such as the Single Net Solution–Remote Deployment Device (SNS-RDD) that uses a spiked net to stop vehicles and the Pre-Emplaced Vehicle Stopper (PEVS) that makes physical contact with a vehicle and injects electricity into it to damage its electronics. At sea, the Maritime Vessel Stopping Occlusion Technologies (MVSOT) entangle propellers.

APPENDIX E

Examples of Game Designs

This appendix describes two hypothetical game designs based on the vignettes listed in Appendix C as a starting point for thinking about how IFCs might be incorporated into future wargames.

Gently Seizing Control of Very Dangerous Weapons: Understanding Risk Perceptions

This is a tactical game based on the vignette "Gently Seizing Control of Very Dangerous Weapons." The objective of this game is to better understand how perceptions of risk affect the decision to employ or not employ IFCs. As described in Appendix C, the game scenario is a NATO raid of a chemical and biological weapon complex held by radical militants planning terrorist attacks. Blue players are tasked with achieving the following:

- conducting extensive intelligence collection regarding the state of the complex
- securely destroying weapon stockpiles and machinery
- collecting small and safe-to-carry items for further analysis
- detaining key personnel for questioning.

Red players are tasked with maintaining control of the complex, safeguarding their weapon stockpiles, and preventing Blue intelligence collection. The basic context of this scenario—a multi-sided civil war in a country on the Mediterranean—is also laid out in the "Gently Seizing Control of the Very Dangerous Weapons" vignette in Appendix C, but additional information, such as international opinion on NATO and the fictional radical group Al-Jabr, is also provided before the game begins. This scenario and context were chosen because the lethally armed adversary, the presence of hazardous materiel, and the imperative for intelligence collection present players with a complex set of risks when using either lethal or nonlethal force.

In this game, the invited players have a mix of expertise on special operations, IFCs, and chemical and biological weapons. Both the Red and Blue teams are acting as platoon commanders, determining how the forces under their command will move, what those forces will target, and how those targets will be attacked (including which capabilities will be used). When making these decisions, both Red and Blue have information on their own capabilities, provided on capability cards included in game read-aheads and game day handouts. Blue has current lethal weapons and IFCs, as well as advanced IFCs, while Red has lethal weapons and current IFCs only. Both teams can also see a map of the complex with locations of forces laid out on it, but only Red is informed of the nature of a given building within the complex until Blue enters or otherwise collects intelligence on that building. Both teams are also provided with their respective rules of engagement.

During each turn, both Red and Blue determine which tactical moves they will make and brief this to the entire group. During this briefing, each team is asked to explain what they expect to accomplish, as well as the risks and benefits associated with their plan of action. The other team is then allowed to comment on the risks and benefits described. As both teams outline their thoughts, the adjudication team interjects whenever player statements appear to conflict with background research on the risks and benefits of IFC use, allowing players to reconsider their arguments or describe why the divergence is justified. When both teams have discussed their moves, the adjudication team determines the move results using dice and probability tables generated from experimental data on each capability in play, potentially modified based on the strength of the arguments presented by each team. Players are notified of the outcomes of their moves and the game map is updated to reflect new unit positions and other relevant information such as infrastructure damage before the next turn begins.

The primary source of data in this game is player discussions of the risks and benefits of using different technologies, as well as how these risks and benefits informed their decisions to use or not use IFCs. This information could be used to guide future work using games or other methodologies. Potential activities might include exploring whether IFC-related risk perceptions are similar in different scenarios or among different demographics, studying highlighted risks in detail to determine whether people's perceptions of IFC-related risk align with actual risk, or considering how to reduce observed misconceptions about IFCs.

Perplexing Perimeter Protection Problems: Exploring Innovative Options

The objective of this game—based on the vignette "Perplexing Perimeter Protection Problems," found in Appendix C—is to identify innovative solutions to the problem of host-nation nationals stealing items from NATO base perimeters. The context of the game revolves around NATO operations to combat extremists in a host nation experiencing high levels of poverty and youth unemployment. This game is based on the 360° game design, so players are provided with a different scenario each turn.[1] While each scenario involves items being stolen from the perimeter of a NATO base, other details vary—such as the level of local extremist activity, opinion of NATO among the populace and local government, identify of the thieves, local social and economic problems, existing base security, and environment surrounding the base.

Players are split into four teams. During each game turn, these teams are tasked with identifying and assessing ways to ensure the security of items on base perimeters. Each team is asked to identify solutions in a different domain: military/technical, informational, diplomatic, or economic. All of the teams are multidisciplinary, containing players with expertise in each of the domains under consideration. Players are primarily making decisions at the level of a base commander or consul-general at a local NATO-member consulate. Because this game is intended to generate innovative solutions, players are not limited to suggesting technologies or procedures currently in use. However, each team is asked to assess the ideas they deem feasible according to a set of measures of effectiveness provided by the adjudication team. After the game, all suggested solutions are also assessed for fitness in solving the problem by the adjudication team using a set of additional criteria. Promising solutions are then explored in more detail using other methodologies, such as prototyping and experimentation.

Although this game does not explicitly incorporate IFCs other than IO, preventing or altering unwanted behavior by unarmed host-nation nationals may be a useful application of IFCs. Including players with expertise on IFCs in the game, and particularly on the team exploring military/technical solutions, would ensure the potential contributions of these capabilities are highlighted when appropriate.

[1] For more information on creating a 360° Game, see Henry, Berner, and Shlapak (2017).

Abbreviations

ADS	Active Denial System
C^{4}ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CONEMP	concept of employment
CONOPS	concept of operations
DoD	U.S. Department of Defense
EW	electromagnetic warfare
IFC	intermediate force capability
IO	information operations
ISR	intelligence, surveillance, and reconnaissance
JIFCO	Joint Intermediate Force Capabilities Office
LOW	Laws of War
M&S	modeling and simulation
MVSOT	Maritime Vessel Occlusion Technologies
NATO	North Atlantic Treaty Organization
NDS	National Defense Strategy
NLW	non-lethal weapon
PEVS	Pre-Emplaced Vehicle Stopper
RFVS	Radio Frequency Vehicle Stopper
ROE	rules of engagement
SAS	System Analysis and Studies
TTPs	tactics, techniques, and procedures
UAV	uncrewed aerial vehicle
VIPER	Vessel Incapacitating Power Effect Radiation

Bibliography

Air Force Doctrine Annex 3-13, *Information Operations*, Curtis E. LeMay Center, Maxwell Air Force Base, April 28, 2016.

Air Force Doctrine Publication 3-12, *Cyberspace Operations*, Curtis E. LeMay Center, Maxwell Air Force Base, November 11, 2011.

Air Land Sea Application Center, *EW Reprogramming*, Curtis E. LeMay Center, Maxwell Air Force Base, February 1, 2011.

Association of Old Crows, *Essentials of Electronic Warfare: What Every Crow Should Know*, 2000.

Beauchamp-Mustafaga, Nathan, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," *China Brief*, Vol. 19, No. 16, September 6, 2019.

Beauchamp-Mustafaga, Nathan, "Exploring Chinese Military Thinking on Social Media Manipulation Against Taiwan," *China Brief*, Vol. 21, No. 7, April 12, 2021.

Christensen, Kyle D., and Peter Dobias, "Wargaming the Use of Intermediate Force Capabilities in the Gray Zone," *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 2021.

Cohen, Raphael S., Nathan Beauchamp-Mustafaga, Joe Cheravitch, Alyssa Demus, Scott W. Harold, Jeffrey W. Hornung, Jenny Jun, Michael Schwille, Elina Treyger, and Nathan Vest, *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*, RAND Corporation, RR-4373/1-AF, 2021. As of June 20, 2022: https://www.rand.org/pubs/research_reports/RR4373z1.html

Crowd Dynamics Modeling Group, Naval Postgraduate School, "Crowd Dynamics Modeling," webpage, undated. As of December 5, 2022:
https://nps.edu/web/crowdmodeling/welcome

Department of Defense Directive 3000.03E, *DoD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy*, U.S. Department of Defense, April 25, 2013, incorporating Change 2, August 31, 2018.

DoD—*See* U.S. Department of Defense.

Field Manual 3-05, *Army Special Operations*, Department of the Army, January 9, 2014.

Hammock, C. J., "Enabling the Development and Deployment of NATO Cyber Operations: An Analysis of Modern Cyber Warfare Operations and Thresholds of Global Conflict," *Journal of Information Warfare*, Vol. 16, No. 3, 2017.

Helmus, Todd C., "7. Social Media and Influence Operations Technologies: Implications for Great Power Competition," *NDU Press News*, November 4, 2020.

Henry, Ryan, Steven Berner, and David A. Shlapak, *Serious Analytical Gaming: The 360° Game for Multidimensional Analysis of Complex Problems*, RAND Corporation, RR-1764-OSD, 2017. As of July 8, 2022: https://www.rand.org/pubs/research_reports/RR1764.html

Joint Air Power Competence Centre, *Joint Air & Space Power Conference 2021: Delivering NATO Air & Space Power at the Speed of Relevance*, Römerstraße, Germany, September 7–9, 2021.

Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)*, July 25, 2018.

Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, January 1, 2021.

Joint Publication 3-12, *Cyberspace Operations*, Joint Chiefs of Staff, June 8, 2018.

Joint Publication 3-13, *Information Operations*, Joint Chiefs of Staff, November 27, 2012, incorporating Change 1, November 20, 2014.

Joint Publication 3-85, *Joint Electromagnetic Spectrum Operations*, Joint Chiefs of Staff, May 22, 2020.

Jones, William M., *On Free-Form Gaming*, RAND Corporation, N-2322-RC, 1985. As of June 20, 2022: https://www.rand.org/pubs/notes/N2322.html

Marine Corps Warfighting Publication (MCWP) 3-32 (formerly MCWP 3-40.4), *Marine Air-Ground Task Force Information Operations*, Department of the Navy, Headquarters U.S. Marine Corps, April 4, 2018.

Mattis, James, *Summary of the 2018 National Defense Strategy: Sharpening the American Military's Competitive Edge*, U.S. Department of Defense, 2018.

NATO—*See* North Atlantic Treaty Organization.

Naval Air Warfare Center Weapons Division, *Electronic Warfare and Radar Systems Engineering Handbook*, NAWCWD TP 8347, 2013.

Navy Warfare Publication 3-13, *Navy Information Operations*, Navy Warfare Development Command, February 1, 2014.

North Atlantic Treaty Organization, *NATO 2030: United for a New Era: Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General*, 2020. As of June 20, 2022: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

North Atlantic Treaty Organization, "Factsheet: NATO Cyber Defence," April 1, 2021.

North Atlantic Treaty Organization, *Intermediate Force Capabilities (IFC): Wargames/Workshops Supporting NATO IFC Concept Development Final Experiment Report*, April 1, 2022a.

North Atlantic Treaty Organization, *NATO 2022 Strategic Concept*, adopted by heads of state and government at the NATO summit in Madrid, June 29, 2022b. As of August 4, 2022: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

North Atlantic Treaty Organization, Public Diplomacy Division, *Active Engagement, Modern Defence: Strategic Concept, Brussels*, NATO, 2010.

Obama, Barack, "U.S. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," The White House, May 1, 2011.

Paul, Christopher, "Understanding and Pursuing Information Advantage," *Cyber Defense Review*, Summer 2020.

Paul, Christopher, Ben Connable, Jonathan Welch, Nate Rosenblatt, and Jim McNeive, *The Information Warfighter Exercise Wargame: Rulebook*, RAND Corporation, TL-A495-1, 2021. As of September 30, 2022: https://www.rand.org/pubs/tools/TLA495-1.html

Paul, Christopher, and Michael Schwille, "The Evolution of Special Operations as a Model for Information Forces," *Joint Forces Quarterly 100*, 1st Quarter, 2021.

Paul, Christopher, Yuna Huh Wong, and Elizabeth M. Bartels, *Opportunities for Including the Information Environment in U.S. Marine Corps Wargames*, RAND Corporation, RR-2997-USMC, 2020. As of June 16, 2022: https://www.rand.org/pubs/research_reports/RR2997.html

Peach, Sir Stuart, "NATO Electronic Warfare and Cyberspace Resilience," presentation at the Joint Air & Space Power Conference 2021: Delivering NATO Air & Space Power at the Speed of Relevance, Germany, 2021.

Perla, Peter P., *The Art of Wargaming: A Guide for Professionals and Hobbyists*, Naval Institute Press, 1990.

Porche, Isaac R., III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy M. Daehner, and Bruce Held, *Redefining Information Warfare Boundaries for an Army in a Wireless World*, RAND Corporation, MG-1113-A, 2013. As of June 20, 2022: https://www.rand.org/pubs/monographs/MG1113.html

Romita Grocholski, Krista, Scott Savitz, Jonathan P. Wong, Sydney Litterer, Raza Khan, and Monika Cooper, *How to Effectively Assess the Impact of Non-Lethal Weapons as Intermediate Force Capabilities*, RAND Corporation, RR-A654-1, 2022. As of June 1, 2022: https://www.rand.org/pubs/research_reports/RRA654-1.html

Rothweiler, Krisjand, "#Wargaming for Strategic Planning," *The Bridge*, March 29, 2017. As of June 14, 2022: https://thestrategybridge.org/the-bridge/2017/3/29/wargaming-for-strategic-planning#_edn6

Savitz, Scott, Miriam Matthews, and Sarah Weilant, *Assessing Impact to Inform Decisions: A Toolkit on Measures for Policymakers*, RAND Corporation, TL-263-OSD, 2017. As of June 17, 2022: https://www.rand.org/pubs/tools/TL263.html

Schwille, Michael, Anthony Atler, Jonathan Welch, Christopher Paul, and Richard C. Baffa, *Intelligence Support for Operations in the Information Environment: Dividing Roles and Responsibilities Between Intelligence and Information Professionals*, RAND Corporation, RR-3161-EUCOM, 2020. As of June 16, 2022: https://www.rand.org/pubs/research_reports/RR3161.html

Theohary, Catherine A., *Defense Primer: Information Operations*, Congressional Research Service, IF10771, December 15, 2020.

U.S. Air Force's Chief Scientist, *Directed Energy Futures 2060: Visions for the Next 40 Years of U.S. Department of Defense Directed Energy Technologies*, FRL-2021-1152, June 29, 2021.

U.S. Department of Defense, *The National Military Strategy for Cyberspace Operations*, Chairman of the Joint Chiefs of Staff, December 11, 2006.

U.S. Department of Defense, *Department of Defense Strategy for Operations in the Information Environment*, June 1, 2016.

U.S. Department of Defense, *2018 Summary Department of Defense Cyber Strategy*, 2018.

U.S. Department of Defense, *Electromagnetic Spectrum Superiority Strategy*, October 1, 2020.

U.S. Department of Defense, "Fact Sheet: 2022 National Defense Strategy," 2022. As of June 20, 2022:
https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF

U.S. Government Accountability Office, *Electromagnetic Spectrum Operations: DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority*, GAO-21-64, December 1, 2020.

Weuve, Christopher A., Peter P. Perla, Robert Rubel, Michael Martin, and Paule V. Vebber, *Wargame Pathologies*, Center for Naval Analyses, CRM D0010866.A1/Final, September 2004.

Wong, Yuna Huh, Sebastian Joon Bae, Elizabeth M. Bartels, and Benjamin Michael Smith, *Next-Generation Wargaming for the U.S. Marine Corps: Recommended Courses of Action*, RAND Corporation, RR-2227-USMC, 2019. As of June 20, 2022:
https://www.rand.org/pubs/research_reports/RR2227.html

RAND NATIONAL DEFENSE RESEARCH INSTITUTE

The U.S. Department of Defense (DoD) and NATO need to be able to assess the tactical, operational, and strategic impact of intermediate force capabilities (IFCs)—a suite of capabilities that cause less-than-lethal effects and whose impact can be difficult to measure. IFCs include non-lethal weapons (NLWs), electromagnetic warfare (EW), cyber defense, and information operations (IO). NLWs include a highly diverse set of systems, including acoustic hailing devices, eye-safe laser dazzlers, flash-bang grenades, rubber bullets, millimeter-wave emitters that cause a temporary heating sensation, microwave emitters that shut down electronics, and entangling devices to stop vehicles or vessels.

The authors build on a previous report in which they described a method measuring the impact of NLWs in the context of DoD strategic goals. This report updates and expands the previous work to encompass all IFCs and to consider both DoD and NATO strategic goals. The authors present logic models (one for DoD and one for NATO) that link use of IFCs with direct outputs, higher-level outcomes, and strategic goals, and they provide vignettes and metrics that help to characterize when and how IFCs have an impact. The authors also discuss how IFCs can be better integrated into wargaming, as well as associated modeling and simulation (M&S), in ways that can facilitate understanding of them and contribute to their integration into DoD and NATO operations.

$37.00

ISBN-10 1-9774-1031-6
ISBN-13 978-1-9774-1031-3

53700

9 781977 410313

www.rand.org

RR-A1544-1