NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

KNOWLEDGE MANAGEMENT APPLICATION TO CYBER PROTECTION TEAM DEFENSE OPERATIONS

by

Alden J. Curnutt and Shandlea R. Sikes

September 2021

Thesis Advisor: Shelley P. Gallup
Second Reader: Brian P. Wood

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE KNOWLEDGE MANAGEMENT APPLICATION TO CYBER PROTECTION TEAM DEFENSE OPERATIONS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Alden J. Curnutt and Shandlea R. Sikes	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The Congruence Model describes the idea that a team can only succeed when the defined components of people, structure, work, and culture all fit together. A key concept of The Congruence Model also identifies the interconnected relationships between components to understand how changes in one area affect performance in others. This model does not, however, include tacit knowledge as a core factor when assessing overall congruency. The research described in this study used data points from real-world Cyber Protection Team member input to build scope-complete behavior models that replicate the pathologies between organization components. Cyber Protection Teams—a subset of teams within the Cyber Mission Force—provided the vehicle to analyze how teams capture, develop, and maintain knowledge in day-to-day defensive cyberspace operations. The intended benefit of our research introduces tacit knowledge as the fifth contributing factor in The Congruence Model to identify prescriptions for knowledge management practices that positively interact with existing components to improve overall organization efficiency.

14. SUBJECT TERMS The Congruence Model, qualitative, Cyber Protection Teams, Cyber Mission Force, cyber protection force	**15. NUMBER OF PAGES** 77
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

KNOWLEDGE MANAGEMENT APPLICATION TO CYBER PROTECTION TEAM DEFENSE OPERATIONS

Alden J. Curnutt
Chief Petty Officer, United States Navy
BS, University of Maryland University College, 2016

Shandlea R. Sikes
Petty Officer First Class, United States Navy
BS, University of Maryland University College, 2019

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED CYBER OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
September 2021

Approved by: Shelley P. Gallup
Advisor

Brian P. Wood
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Congruence Model describes the idea that a team can only succeed when the defined components of people, structure, work, and culture all fit together. A key concept of The Congruence Model also identifies the interconnected relationships between components to understand how changes in one area affect performance in others. This model does not, however, include tacit knowledge as a core factor when assessing overall congruency. The research described in this study used data points from real-world Cyber Protection Team member input to build scope-complete behavior models that replicate the pathologies between organization components. Cyber Protection Teams—a subset of teams within the Cyber Mission Force—provided the vehicle to analyze how teams capture, develop, and maintain knowledge in day-to-day defensive cyberspace operations. The intended benefit of our research introduces tacit knowledge as the fifth contributing factor in The Congruence Model to identify prescriptions for knowledge management practices that positively interact with existing components to improve overall organization efficiency.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAR	After Action Report
ADCON	Administrative Control
AOR	Area of Responsibility
ARCYBER	U.S. Army Cyber Command
CCMD	Combatant Command
CMF	Cyber Mission Force
CONOP	Concept of Operations
COPS	Current Operations
CPF	Cyber Protection Force
CPT	Cyber Protection Team
CTE	Cyber Threat Emulation
CTN1	Cryptologic Technician (Networks) Petty Officer First Class
CTNC	Cryptologic Technician (Networks) Chief Petty Officer
DCI	Discovery and Counter Infiltration
DCO	Defensive Cyberspace Operations
DMSS	Deployable Mission Support System
DOD	Department of Defense
DODIN	Department of Defense Information Networks
Dr.	Doctor
E	Enlisted
FOPS	Future Operations
Ft	Fort
ICC	Intermediate Cyber Core
IDE	Integrated Development Environment
IP	Internet Protocol
JCS	Joint Chiefs of Staff
JQR	Job Qualification Requirement
KM	Knowledge Management
LL	Lessons Learned
ME	Mission Element

MEL	Mission Element Lead
MP	Monterey Phoenix
MPT&E	Manpower, Personnel, Training, and Education
Mr.	Mister
MTE	Man, Train, and Equip
NPS	Naval Postgraduate School
NRP	Naval Research Program
O	Officer
OIC	Officer-in-Charge
OJT	On the Job Training
OPCON	Operational Control
OPNAV	Office of the Chief of Naval Operations
POR	Program of Record
TCM	The Congruence Model
TK	Tacit Knowledge
TL	Team Lead
U.S.	United States
USCYBERCOM	United States Cyber Command
USINDOPACOM	United States Indian Ocean Pacific Command
USN	United States Navy

ACKNOWLEDGMENTS

The authors would like to thank the following people for the assistance and support provided throughout the capstone process.

- Dr. Shelley Gallup, from Naval Postgraduate School (NPS), for his incredible guidance and support as advisor throughout the entire process of the project.
- Mr. Brian Wood, from NPS, for both his relentless pursuit of excellence and equal support as the second reader.
- The five Navy Pacific Cyber Protection Teams for supporting the research effort with participation and senior enlisted leaders who made that facilitation possible.
- Most importantly, our families, significant others, and children for their limitless love and support through the many hours spent working on this project.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

"Knowledge is regarded as a fluid mix of framed experiences, values, context, insight, and intuition" (Davenpooty & Prusak, 1998). Knowledge Management (KM) provides a framework for creating, promoting, and sharing knowledge. The subsequent accumulation and distribution of knowledge is a crucial variable in the success of an organization. The analysis of knowledge and *how* organizations use it become more efficient and effective is an important area of study. For the U.S. military, knowledge discipline area has proven to be a complex and persistent challenge. The Congruence Model (TCM), developed in the 1980s by David A. Nadler and Michael L. Tushman, frames the bond between the core factors of an organization to identify methods for performance improvement (Janse, 2019). TCM—displayed below in Figure 1—identifies and correlates critical elements of an organization's people, the work they do, structure in which they operate, and the resulting culture. The application of these internal components lies at the heart of our research.

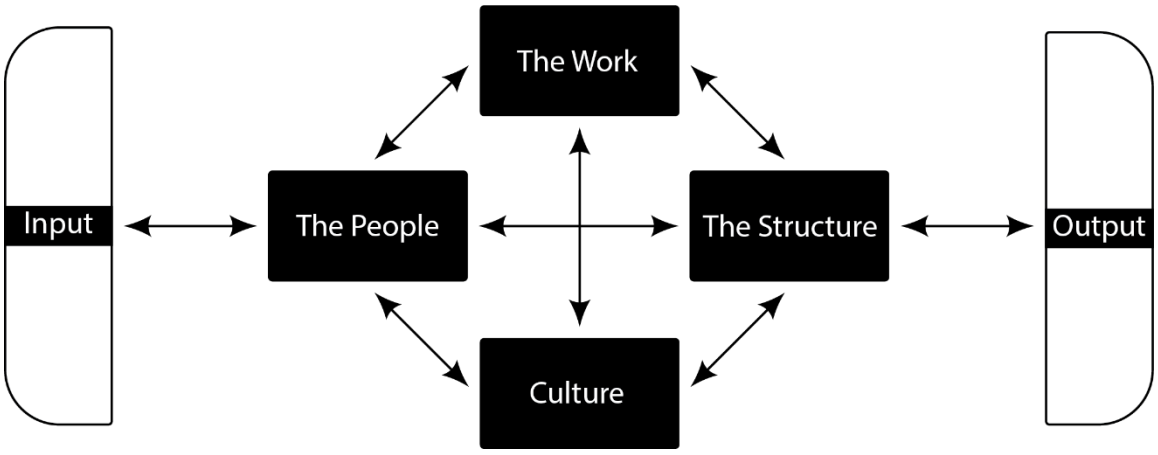


Figure 1. The Congruence Model. Source: Mercer Delta (1998)

In 2012, the Joint Staff and Commander, United States Cyber Command (USCYBERCOM) directed the armed services to build the Cyber Mission Force (CMF), a

distributed effort consisting of approximately 6,100 joint military personnel operating across 133 teams to direct, synchronize, and coordinate cyberspace operations (ARCYBER, 2020). Figure 2 captures a visual summary of the Cyber Mission Force organization chart.

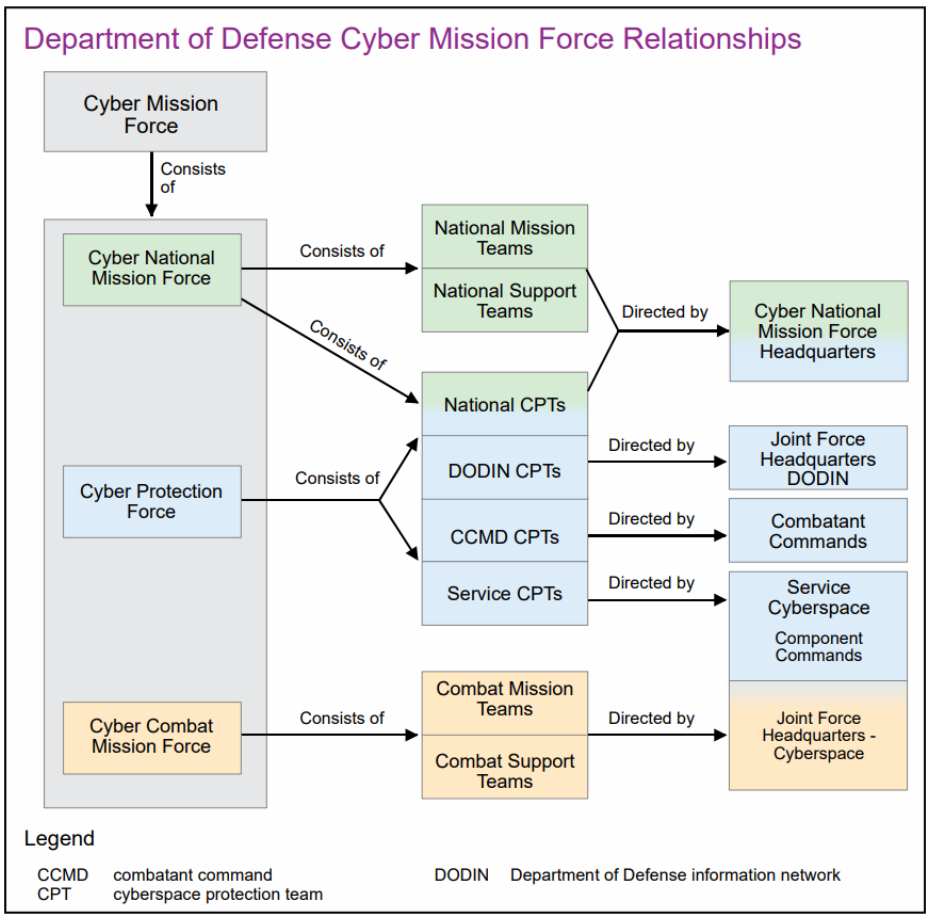


Figure 2. Department of Defense Cyber Mission Force Relationships. Source: JCS (2018).

Cyber Protection Teams (CPTs), a tactically focused subset of teams collectively referred to as the Cyber Protection Force (CPF), were tasked in part with the defense of friendly cyberspace networks, data, and capabilities. CPTs play a critical role in the Department of Defense's (DOD's) defense-in-depth strategy. CPT personnel are routinely

organized into small groups (5-7 members) called Mission Elements (ME) that conduct essential network security assessments for U.S. military networks around the world.

A CPT's ability to conduct defensive cyberspace operations involves a complex mesh of knowledge areas which may be difficult or impossible to codify. The heart of our research lies within the challenges faced by CPTs which balance both billet manning and knowledge retention in the execution of defensive cyberspace operations. This connection ultimately bridges the gap between the issues impact the CPF and our study of tacit knowledge as an additional core factor in TCM.

B. PURPOSE / SIGNIFICANCE OF RESEARCH

Explicit knowledge is the most common and formal way to transfer knowledge in both verbal and written forms. Alternatively, tacit knowledge gained through personal experience and perspective is extremely difficult to transfer from one person to another. Cyber Protection Teams face this relentless challenge while manning, training, and equipping team personnel for missions across the globe. There is a noticeable gap between the retention efforts of explicit and tacit knowledge bases in the teams. In particular, knowledge is lost when members depart from a CPT without an effective way to transfer their hard-earned experience to other personnel. The lack of comprehensive tools or approaches needed to maintain and implement organizational effectiveness negatively impact CPT training and mission execution. These points were synthesized to form our two research questions:

1. How does the inclusion of tacit knowledge into The Congruence Model impact the model's determination of organizational fit and performance?
2. How can tacit knowledge be measured within the Cyber Protection Team's as a method to test its inclusion into The Congruence Model?

We approached these questions using our research and understanding of knowledge to develop tailored questionnaires that were completed by fourteen members across five CPTs in the Pacific theater. This data was analyzed to determine the value and flow of tacit knowledge, the impact of its loss, and its potential to measure organizational congruence.

The four tenant concepts of the Congruence Model are processes, organization, personnel, and technologies. Using these elements, we analyzed the Protection Teams to understand the core work that occurs and pathologies that develop between internal components. We hypothesized that tacit knowledge could be measured and applied as part of TCM to identify the inefficiencies of an organization and prescribe relevant solutions.

C. SCOPE

The scope of this research focused on the internal components of a CPT's work, people, and structure to identify pathologies and / or barriers related to knowledge flow. The input, output and culture were excluded from our research to focus on the internal pieces within each team. Analysis was conducted on real-world pathologies that develop between CPT personnel, the work they do, and the structure in which they operate. The goal of our research was to frame, analyze, and model the teams to understand how tacit knowledge affects organization performance. This thesis is supported by Naval Postgraduate School (NPS) as a subproject within the Naval Research Program (NRP), sponsored by OPNAV N1-Manpower, Personnel, Training, and Education (MPT&E), Developing a Formal Knowledge Management (KM) Process (Nissen & Gallup, 2013).

D. THESIS ORGANIZATION

This research is organized as follows:

- Chapter II covers the literature review for knowledge and knowledge relationships, an in-depth look at The Congruence Model, and relevant information about Cyber Protection Teams.
- Chapter III identifies the methodology of our data collection and three-stage analysis used to analyze that data.
- Chapter IV discusses how each stage of analysis was used each to identify the presence of tacit knowledge flows and potential barriers.

- Chapter V provides our recommendations, study limitations, and promising areas for future research of tacit knowledge.

E. BENEFITS OF STUDY

This study revealed the benefits of KM application through The Congruence Model to analyze and identify organizational inefficiency. This research also identified the qualitative benefit to organizational modeling with the inclusion of tacit knowledge as a core contributing factor in TCM. Further benefits of this study examined the commonalities of the knowledge flow pathologies within the sampled CPTs by identifying barriers that affect knowledge transfer and retention.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

This chapter reviews the literature and background for knowledge / knowledge relationships, an in-depth look at The Congruence Model, and relevant information concerning Cyber Protection Teams. This research focused on understanding the role of tacit knowledge as an additional core component of The Congruence Model to measure organizational congruence of Cyber Protection teams who perform defensive network assessments. As a Title 10 unit, Cyber Protection Teams conduct military operations despite high rates of personnel turnover. Understanding the connection between defensive operations and the intra-personal cohesion was a vital step our effort to understand how knowledge manifests and with what value.

This research focused on understanding the role of tacit knowledge as an additional core component in The Congruence Model. The paradigm of personnel loss experienced by Cyber Protection Teams provided an excellent opportunity to analyze the fundamental value of knowledge and knowledge flow within real-world organizations. As a side effect, the outcome of this research exposed prescriptions to limit knowledge loss as personnel rotate out of CPT billets.

A. KNOWLEDGE AS A DOMAIN

1. Defining Knowledge and Its Boundaries

Before exploring the value and impact within a CPT, it is important to first establish the foundational concepts of knowledge. The *Merriam-Webster Dictionary (online)* defines knowledge as 1. a) "the fact or condition of knowing something with familiarity gained through experience or association" b) "the range of one's information or understanding." 2. a) "the sum of what is known; the body of truth, information, and principles acquired by humankind" (2021). Biggam (2001) extends this definition by stating that "knowledge can be gained through experience [as well as] rational thought" (p. 7). This latter idea provides a realistic perspective in the context of human communication. The rationale also reveals the human potential to leverage existing bodies of knowledge to create, build, or understand a topic. In the wide-ranging field of technology, for example,

it is unnecessary to build an integrated circuit from raw components in order to understand the functions of digital logic. Analogously, knowledge can be acquired through the study of information which already exists.

Defining knowledge and understanding its acquisition is largely an exercise rooted in means rather than ends. It is useful to analyze what combination of factors constitute knowledge as much as what that constitution enables (or disables when absent) as a result. The core of this idea exists in the "knowing-doing gap" which describes a delta between an acquired body of knowledge and how it translates to action or output (Esler et al., 2010). A logical assumption, for example, could be made that collecting and disseminating knowledge to all parts of an organization will lead to meaningful change. Pfeffer and Sutton (1999) identify two problems with this pattern: 1) "knowledge is something explicit and quantifiable" and 2) it is "a tangible good and the use of that good in ongoing practice" (p. 85). These points highlight a subtle, yet important distinction. Knowledge, regardless of source, must be both useful and employed to offer the sharpest competitive edge. Simply put, knowledge enables action but does not guarantee it.

2. The Evolution and Flow of Knowledge

The topic of knowledge is nuanced and understanding without practical application may lead to the conclusion that it is a naturally occurring phenomenon. This conclusion, however, betrays the relationships necessary for knowledge to exist. Nissen recognized these relationships—covered in Harnessing Dynamic Knowledge Principles in the Technology-Driven World –between data, information, and knowledge as an actionable / abundance hierarchy (Nissen, 2013). Data has the lowest actionability and highest abundance in this hierarchy, serving to remove uncertainty about a circumstance. Compiled data which enables meaning through context marks the transition to information. Collections of information that enable action mark the final transition to knowledge. Analyzing these layers in the context of a defensive cyberspace vignette underscores salient characteristics about each.

Data is not actionable, but it is abundant. Within our vignette, data points include atomic values—values which cannot be further simplified—such as an IP address, a binary

value, or an individual database transaction. These points are valuable to defensive operations but do not indicate a requisite action. Data becomes information when it begins to enable understanding. Processing data to associate an IP address with a malicious source, for example, marks the transition from data into information as defensive operators begin to understand the state of a network, but are not necessarily prepared to act. Although less abundant than data or information, knowledge balances understanding with courses of action that best support an end goal. Pairing mitigation techniques with network vulnerabilities provides an informed way to act. The vignette's inclusion of atomic data points, malicious source characterization, and compatible response capabilities display key characteristics at each layer of the actionable / abundance hierarchy.

3. Relationships between Tacit Knowledge and Explicit Knowledge

A foundational understanding of knowledge enables the exploration of its characteristics. While tacit and explicit knowledge are *both* forms of knowledge, they are characterized differently. Most explicit knowledge ("know-what") is articulated and codified in formal language, manifest in organizational procedures or policies. CPT-specific examples of this come in the form of, among others, standard operating procedures, defensive tool documentation, and customer network diagrams. These "explicit knowledge assets can be reused to solve many similar types of problems or connect people with valuable knowledge" (Smith, 2001). The recordable, transferable characteristics of explicit knowledge reduce the friction of information sharing and allow it to flow with relative ease.

Tacit knowledge, however, is "difficult to articulate in writing and is acquired through personal experience." (Hansen et al., 1999). The maturation of this knowledge drives an individual's intuition and common sense, enabling a deeper understanding of a task. This internalization improves one's ability to differentiate between courses of action ("know-how") to determine the best response. This deep-rooted, actionable nature of tacit knowledge translates to an extremely valuable resource for organizations (Ambrosini & Bowman, 2001). This holds true for CPT assessments largely conducted on large, complex networks. Timely execution of these assessments relies, in part, on the team's ability to

leverage its aggregated tacit knowledge to operate efficiently and effectively. Despite its demonstrable importance, however, this knowledge transfers more slowly than its explicit counterpart. Resistance to articulation may also mean that an organization has not codified the full scope of knowledge required for its members to accomplish all of its tasks.

An example involving the Cyber Protection Teams described above is a useful exercise to frame the difference between explicit and tacit knowledge. *That* Cyber Protection Teams conduct defensive cyberspace operations is explicit knowledge that can be defined, expressed, and understood. In contrast, the ability to conduct *effective* defensive operations involves a complex mesh of professional development and personal experience. Enlisted members largely undergo formal training before onboarding with a Protection Team. It is reasonable to conclude that upon arrival after successful completion of training, personnel largely understand the basics of digital networking. Explicit knowledge of routing protocols and cyberspace tool documentation enables an operator to perform necessary tasks. In turn, tacit knowledge backed by experience enables tasks to be executed efficiently and effectively. While tacit and explicit knowledge both have value, these examples demonstrate key differences and reflect systematic issues faced by CPTs across the CPF.

B. THE CONGRUENCE MODEL

1. Overview of The Congruence Model

The Congruence Model is centered around the Contingency Theory that was developed in the early 1980s by organizational theorists David Nadler and Michael Tushman. Nadler and Tushman's TCM characterizes interactions between processes, organizations, personnel, and technologies. This open system modeling approach to organization performance can be used to observe inputs and resulting output. The introduction of knowledge into the model is a natural fit, as it exhibits a bi-directional flow between members of a team, similarly to existing components. The term pathology (singular) or pathologies (plural) accurately describes this flow as a phenomenon that both effects and is affected by other factors in an organization. As a result of its application, the model can detect the sources of performance gap barriers that prevent fundamental change.

As a method for contingency planning, TCM can also help organizations observe and subsequently function in operationally degraded environments.

TCM, as with all models, does have limitations. The internal focus on congruence may not account for external factors that unevenly affect internal components. Furthermore, this model can be used to identify performance inefficiencies but not necessarily *how* to fix any problems that are discovered.

2. Analysis of TCM Current Concepts

There are four tenant concepts of The Congruence Model that work in unison: processes, organization, personnel, and technologies. Initial application of the model enables analysis and understanding of the core work accomplished by an organization's people. The subsequent analysis of critical processes can help identify the factors that affects the bi-directional relationships between components. Finding and studying each unique challenge can ultimately lead to the discovery of resolutions that solve incongruities and improve overall efficiency. The summary of our goal was to understand where the core work was being accomplished, by whom, and when.

3. Congruence Analysis through Behavior Modeling

The application of TCM provides an effective way to frame the components of an organization. However, there are no universal methods to quantitatively measure the congruence of those framed components. Monterey Phoenix (MP), a project developed by Dr. Mikhail Auguston at the U.S. Naval Postgraduate School in Monterey, California, uses a high-level, executable language with an event-driven syntax to model complex behaviors within a system. The intelligent design of MP combines a code-like event grammar with an expressive syntax that can replicate real-world behavior with human readable values. MP was chosen to measure and evaluate scope-complete permutations of network assessments conducted by CPT personnel.

C. CYBER PROTECTION TEAMS

1. CPT Overview and Mission Focus

In 2012, the Joint Staff and Commander, United States Cyber Command (USCYBERCOM) directed the armed services to build the Cyber Mission Force (CMF), a distributed effort consisting of 6,100 joint military personnel operating across 133 cyber teams to direct, synchronize, and coordinate cyberspace operations (DOD, 2016). Cyber Protection Teams (CPTs), a tactically focused subset of teams collectively referred to as the Cyber Protection Force (CPF), were tasked in part with the defense of friendly cyberspace networks, data, and capabilities.

Pursuant to these assigned objectives, CPTs function as a globally distributed layer of protection in the DOD's defense-in-depth strategy. Each CPT is billeted for 39 personnel and routinely deploys small 5–7 person teams, called Mission Elements, to perform complex network assessments. These assessments determine each surveyed customer's level of defensive posture and preparedness. Subsequent reports provide vital network litmus tests to both the customer organization and corresponding cybersecurity providers throughout the enterprise (Trent et al., 2019).

2. Organizational Turnover

Military services largely share a culture of high workforce turnover due to limited tour durations. The average length of time spent on orders at one CPT is 36 months. Personnel spend approximately three to six months acclimating to the new team after arrival and three months of preparation prior to departure, with the greatest contribution to mission and objectives occurring between the two time frames. Over the course of a tour, both officer and enlisted personnel focus on one or more areas of defensive network analysis. In the context of a CPT, turnover is a term used to describe the process in which more experienced personnel relay a wide range of topics about the team that span both explicit and tacit knowledge formats. Personnel who arrive as relief (individuals replacing departing members who have both the required rank and requisite level of training) for

members who have already departed are not offered the opportunity to conduct this process.

3. Protection Teams and Knowledge Context

Tacit knowledge enables a unique understanding within an organization's mission area. The highly dynamic nature of cyberspace, its impact on stakeholder organizations, and relevant information required to operate are inextricably connected. These factors affect how knowledge is used to solve domain-specific problems. For example, *that* USCYBERCOM is a functional combatant command is explicit knowledge that can be defined, expressed, and understood by a recipient. However, the *ability* to conduct effective cyberspace operations involves a complex mesh of knowledge areas. The heart of this research lies within the challenges faced by CPTs which balance both billet manning and knowledge retention to execute defensive cyberspace operations. This connection ultimately bridges the gap between our study of knowledge and what role it plays in an organization.

D. KNOWLEDGE AS A MEASURABLE PHENOMENON

The role of knowledge plays a clear and present role in the Cyber Mission Force. Despite the action it enables, characteristics of knowledge also make it difficult to accurately quantify and capture. This is particularly true regarding tacit knowledge – a fact many Protection Teams struggle to reconcile with the rate of personnel turnover. This reality highlights a similar challenge to our research as it explored organizational congruence, including tacit knowledge as an additional factor for TCM analysis.

1. Introduction of the Physical World

The measurement of phenomena in the natural world has long been used as a scientific vehicle to understand the processes around us. Returning to Merriam Webster, phenomena is defined as: "an object or aspect known through the senses rather than by thought or intuition" and "a fact or event of scientific interest susceptible to scientific description and explanation" (2021). In the field of physics, energy measures the value that must be transferred to an object to perform a unit of work. Moreover, the binary states of

potential and kinetic energy subdivide this measurement. Consider a rubber band that is stretched. The potential for energy inside the rubber band increases as the band is stretched while releasing it converts the potential energy into kinetic movement. Similarly, the potential to accomplish work in a team grows as task-relevant knowledge is reflected in individual experience. Performing an action represents the transformation into kinetic energy as knowledge is used to execute a task.

An extension of energy, entropy "measures the energy degradation in a natural system through increasing disorder" (Andriessen & Bratianu, 2008). Higher values of entropy indicate lower values of measurable energy. Entropy can be reduced by introducing rigor to a system. A highly organized top-down structure of a Protection Team, for example, reduces the entropy values associated with knowledge loss. The human brain is significantly less rigid when compared to traditional military organization. Consequently, tacit knowledge, largely based on individual experience and subjectivity, naturally exhibits higher values of entropy than explicit knowledge. The measurability of energy and entropy can help us quantify knowledge and accurately extract its value to an organization.

2. Connections Between Knowledge and the Physical World

Although knowledge is difficult to measure through traditional human sensing, it "can be observed through the relationship between knowledge and the behaviors associated with knowledge" (Simms & Johnson, 2012). Knowledge as a phenomenon in the context of a CPT means analyzing not only the outcomes of task-oriented work, but also the intangible culture that manifests as a result between team members. Actionability is key in this observation. Pfeffer and Sutton highlight that even though "superior [knowledge] management practices are reasonably well known, diffusion proceeds slowly and fitfully, and backsliding is common" (Pfeffer & Sutton, 1999). The fact that knowledge is critically important to organizational success, yet resistant to effective capture is perhaps the greatest force driving the use of other domains and disciplines to measure the value of knowledge.

III. METHODOLOGY

This chapter describes the methodology used to frame Cyber Protection Team operations for data collection and behavior modeling. The research effort was organized and concentrated into three distinct parts:

1. The Congruence Model was used to frame the internal components of CPTs to understand:

   a) The fundamental tasks accomplished in each CPT that underpin the event phases of defensive network assessments

   b) How the members of each team complete that work

3. Anonymous questionnaires, distributed to personnel across three distinct demographics were used to identify how tacit knowledge is used to accomplish work and how that knowledge is transferred between teams and team members.

4. Monterey Phoenix, an executable, event-driven programming language, was used as an iterative, scope-complete behavior modeling platform to quantitatively measure tacit knowledge barriers to team personnel in the five event phases of network assessments.

1. The Internal Components of Cyber Protection Teams

Cyber Protection Teams were designed and staffed with the same institutional structure found throughout the U.S. military. Top-down or reverse-pyramid hierarchies, one form of many organizational structures, have historical significance when analyzing the relationships between members, the work done by these members, and strategic direction. Mercer Delta—an asset management and consulting firm—acknowledged this precedence, stating the inherent challenges in which "the rapidly accelerating pace of change has made that static model obsolete" (Mercer Delta, 1998). The distribution of authority in this perspective grants decision-making power to those at the top of an organization that disproportionately affect subordinates. As a result, leaders operating in

this paradigm my not fully understand the full effect of those decisions on subordinate members. Although CPTs fall within the military Cyber Mission Force structure, the team-of-teams Mission Element approach to network assessments and the range of expertise on each team indicate nuanced organizational details. This research categorized CPTs into the three in-scope components that coexist to form the transformation process at the heart of TCM:

- its people
- the work they do
- the formal structure

2. Scope

Two research questions were developed to understand tacit knowledge and how it affects an organization:

1. How does the inclusion of tacit knowledge into The Congruence Model impact the model's determination of organizational fit and performance?
2. How can tacit knowledge be measured within the Cyber Protection Team's as a method to test its inclusion into The Congruence Model?

With the understanding that tacit knowledge enables action and "no practical organization can function without the individuals and groups of people in it," (Nissen, 2014) the methods of this research focused on CPT operators (the people) and network assessments (the work) they perform. By design, the culture component of TCM was excluded from the scope of this research to limit complexity during behavioral modeling discussed later in this chapter.

Network assessments are the primary mission focus for CPTs. Given the dynamic and complex nature of these networks, actionable knowledge enables each Mission Element to successfully navigate the customer-evaluator relationship from start to finish. This knowledge-rich environment became the focal point our research. The assessment process was divided into five event phases with corresponding event actors as referenced

in Table 1. Clearly defined event phases and actors allowed us to isolate the relevant TCM components for each pathology in order to test and observe the resulting behavior in the form of MP event traces. The use of "event" for each segment in the assessment process was intentional and is discussed later in this chapter with Monterey Phoenix.

Table 1. CPT Network Assessment Events and Assessment Personnel

	Assessment Personnel				
Assessment Events	**Team Lead**	**Cyber Planner**	**Mission Element Lead**	**♦Mission Element Operator**	**♦♦Defensive Analyst**
Assessment Scheduling	x				
Initial Site Survey	x	x	x		
Assessment Planning & Staffing	x	x		x	
Assessment Execution		x		x	x
Post-Assessment Action	x			x	

♦Selected based on assessment requirements from a Site-Survey
♦♦Advisory role to the Team Lead and Mission Element Lead

B. ANONYMOUS QUESTIONNAIRES

1. TCM and CPTs: The Connective Tissue

The role of CPTs as defensive cyberspace assessors in the Cyber Mission Force is largely stable and has not changed since the CPT's inception in 2010. While the composition of networks can differ among organizations and even operational theaters, mission objectives are team-agnostic across the Cyber Protection Force. Individual members, however, contribute to this mission with unique tacit knowledge, individually shaped by personal experience. Questionnaires were developed and distributed to personnel with a wide range of experience and paygrade across five Pacific Theater CPTs to gather qualitative feedback. The teams and their geographic locations are listed in Table 2. The questionnaire process and member input were conducted anonymously,

communicating through two senior enlisted leaders who serve as operational managers for the teams. Names or personal information were excluded from the data collection process to prevent attribution for any participant.

Table 2. CPT Sample Frame

CPT Sample Frame	
Team Name	Geographic Location
500 CPT	Oahu, Hawaii
501 CPT	Oahu, Hawaii
502 CPT	Oahu, Hawaii
551 CPT	Oahu, Hawaii
553 CPT	San Diego, California

2. Questionnaire Composition

A total of nine questions, as seen in Figure 3, were designed to reveal the connections between CPT personnel and the work they perform as modeled with TCM. The questions prompted team members for input regarding (1) the objectives of CPT operations from the team member point of view, (2) the formal training pipelines that prepare personnel for CPT billets, (3) the use of both formal and tacit knowledge to prosecute objectives, and (4) the methods CPTs use to transfer knowledge between personnel to include on-the-job training, turnover processes, and lessons learned. All four question categories used in this research were designed to target core areas where the use of tacit knowledge was likely to affect organization performance. Identifying member experiences in these areas informed our understanding of the influence and constraints of behaviors within the sampled environment.

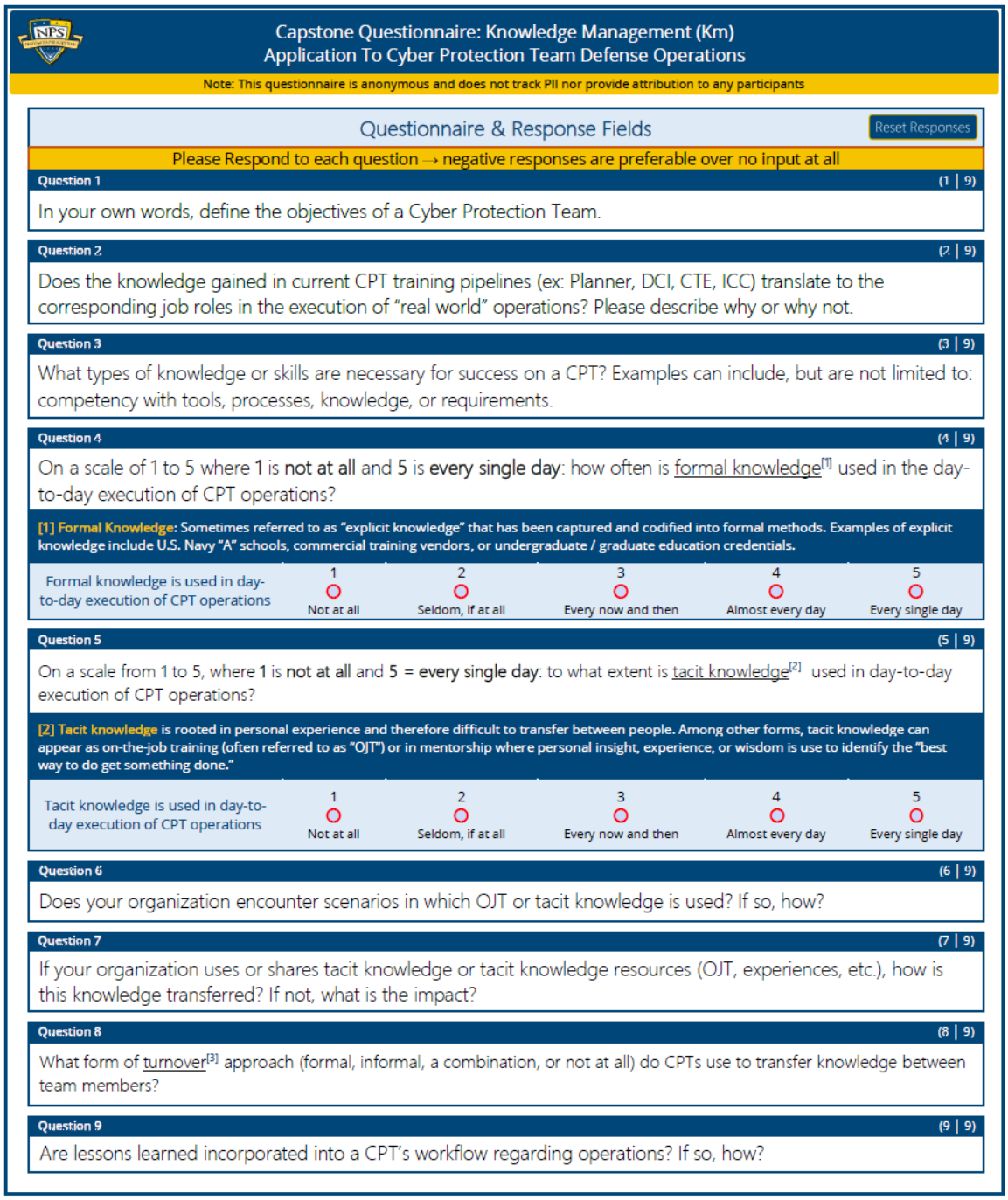


Figure 3. CPT Personnel Questionnaire

C. MONTEREY PHOENIX BEHAVIOR MODELING

1. An Introduction to Monterey Phoenix

To answer the second research question regarding the measurement of tacit knowledge within CPTs, the research methodology used Monterey Phoenix (MP) to model behaviors of CPT personnel during network assessments. Monterey Phoenix, A project developed by Dr. Mikhail Auguston at the U.S. Naval Postgraduate School in Monterey, California, uses a high-level, executable language with an event-driven syntax to model complex behaviors within a system. Words appearing `IN THIS FORMAT` will reference MP-specific terms and keywords used within the platform's source code. Network assessments and relevant assessment stakeholders were mapped to models that were then executed in the MP environment to observe scope-complete behavior representing the work that underpins the entire assessment process.

2. Modeling the Protection Teams

All events in a single model are organized into one `SCHEMA` with each event defined as a child to the `SCHEMA` in its own unique `ROOT` scope with associated characteristics. For example, site surveys of a network are defined as a `ROOT` event under the `Network_Assessment SCHEMA`, must `PRECEDE` the `Assessment_Preparation ROOT` event, but `INCLUDE` vital steps such as completing target `Network_characterization` and `Survey_coordination` with the customer organization. Source code used to translate CPT assessments into Monterey Phoenix events is described in Chapter IV and displayed in Appendices A–C. Executing defined models in MP result in one or more *traces*—the term used in Monterey Phoenix to describe one permutation of possible output—per model. Trace outputs from each executed model were analyzed to characterize the quantitative behavior of events with and without tacit knowledge constraints.

IV. ANALYSIS

The findings in this chapter are a result of our three-stage analysis. The first stage of analysis describes how Cyber Protection Teams were framed with The Congruence Model to understand the role of internal components and their bi-directional interaction. The second stage discusses how respondent answers, gathered via questionnaires, were categorized and distilled into seven distinct tacit knowledge flows. The term pathology (singular) or pathologies (plural) will be used in this chapter to identify the transfer of knowledge from one internal component to another. The final stage of analysis describes how the identified components of CPTs were overlaid with the seven discovered pathologies to produce executable code for Monterey Phoenix that resulted in iterative, scope-complete behavior models.

A. FRAMING NETWORK ASSESSMENT EVENT PHASES

As summarized in Chapter II, The Congruence Model provides a flexible method to frame an organization into three related pieces that affect overall congruence:

- **Input** to the organization including external environmental factors or forces applied from other organizations / people.
- **Internal components** in a meshed symbiosis of people, work, structure, and culture as key drivers of performance.
- **Output** from the organization as a result of the internal components working together to operate on the received input.

This system of systems model reflects the interconnectedness between components where a change in one affect one or more pieces of the organization. Our sample frame was modeled using a modified approach to TCM, visually captured in Figure 4 with a focus on the internal components of work, people, and structure. The input, output and culture were excluded from our research to focus on the internal presence and flow of tacit knowledge within each team. Analysis was conducted on real-world pathologies that develop between CPT personnel, the work they do, and the structure in which they operate. These

components collectively affect team congruence throughout every phase of a network assessment.

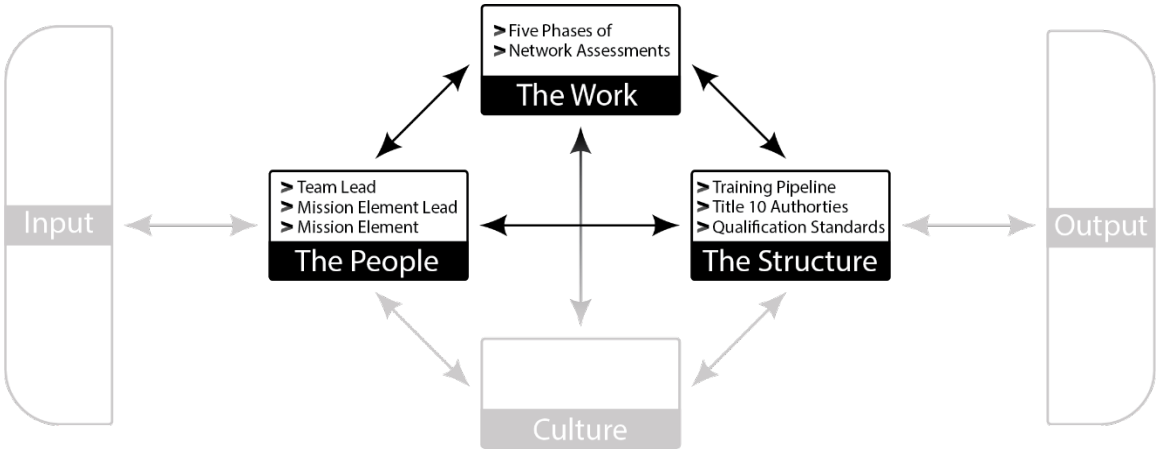


Figure 4. The Scoped Components of The Congruence Model

Initial analysis identified the elements of Protection Teams and mission areas that translate to TCM core components. This translation can be seen in Table 3 along with a summary list of each pertinent component.

Table 3. TCM Model Component Translation to Cyber Protection Teams

TCM Component	Related CPT Component	Component Examples
The People	Relevant stakeholders in the network assessment process	Team Lead Mission Element Lead Cyber Planner Mission Element Operators External Stakeholders
The Work	CPT Network Assessments and administrative reporting	Five phase-network assessments After-Action Reports
The Structure	Operational Title 10 relationships	Operational Control (OPCON) Administrative Control (ADCON)

1. The People: Network Assessment Stakeholders

Tacit knowledge, as described in Chapter II, is a phenomenon that occurs in and between the people of an organization. As a key component in the context of both TCM and defensive cyberspace assessments, CPT work roles were analyzed using Job Qualification Requirement (JQRs) documents—work role-specific training support that guides each team member's explicit and tacit knowledge development while with a team – to identify how and where each fit into the overall organization. A summary of key stakeholders is listed below.

Internal CPT Personnel

- **CPT Team Lead** (Abbreviated as TL): Individuals who function as the primary connective tissue between the operators who conduct the assessment, the assessment itself, and the Protection Team's highest-ranking officer, or Officer in Charge (OIC). The level of coordination and interaction with superior commands / ranking officials—such as higher headquarters, government officials, joint military organizations, and multinational partners—necessitates the fulfillment of these work roles by officers ("JQR for DCO Team Lead Basic," p. 2).

- **CPT Mission Element Lead** (Abbreviated as ME Lead or MEL): Individuals appointed on a per-mission basis to provide tactical, first-line leadership to Mission Element operators before, during, and after the assessment process. This work role is considerably more flexible than that of the TL, where practical experience and qualification status are considered equal factors to paygrade. This flexibility enables a dynamic range of eligible personnel to fulfill this role from E-6 through O-2.

- **CPT Cyber Planner**: Individuals who perform vital functions throughout the assessment process which involve coordination with CPT leadership / higher headquarters elements, tracking and planning Future Operations (FOPS), and Current Operations (COPS) support to activated ME teams. Members filling the Cyber Planner work role are typically experienced in

two or more CMF work roles across both defensive and offensive missions sets ("JQR for DCO Planner Basic," p. 3).

- **CPT Mission Element Operators**: Individuals who staff the five to seven person Mission Elements on a per-assessment basis; this number can rise or fall depending on the size of a target network. Operators constitute the majority of a CPT's 39 total positions and collectively represent a wide range of skills and experience. In ideal circumstances, each Mission Element is staffed with Operators who have skillsets that correspond to the results and recommendations of a network's site-survey.

External Stakeholders

- Commander, Operational Higher Headquarters: CPTs were developed as small, tactical teams without designation as a standalone military command. A superior commander exercises Operational Control (OPCON)—the authority exercised by a military commander to direct mission-related tasking for subordinate units—of Protection Teams within a defined Area of Responsibility (AOR), interfacing with CPT leadership / planning staff to delegate mission planning and requirements.

- Mission Owner: The individual within a customer organization designated as the primary point of contact for the duration of a CPT assessment, with most interaction occurring during the Site-Survey and Assessment Execution phases described in the next section.

- Program of Record Owner: The primary point of contact for a Program of Record (POR) whose assets reside on a customer's internal network. These tenant programs typically provide unique capabilities to one or more organizations and can introduce additional requirements for the Site-Survey team. POR Owners are functionally subordinate to the Mission Owner over the span of network assessments event phases.

2. The Work: CPT-Customer Network Assessments

Performing network assessments constitute one of the primary Protection Team mission focus areas. The modular nature in which Mission Elements are staffed and deployed requires a level of autonomy backstopped by actionable knowledge. These characteristics made the process a prime candidate to analyze the presence, flow, and effect of knowledge flow pathologies. The assessment process was subsequently mapped to five self-contained event phases, as seen in Figure 5. In some cases, Efforts within some event phases can be concurrently completed but each occurs sequentially without condition. This linear mapping enabled MP logic to reflect the tacit knowledge relationships between **ROOT** events in terms of positive and negative reinforcement. The five event phase are listed below with the associated milestones for each.

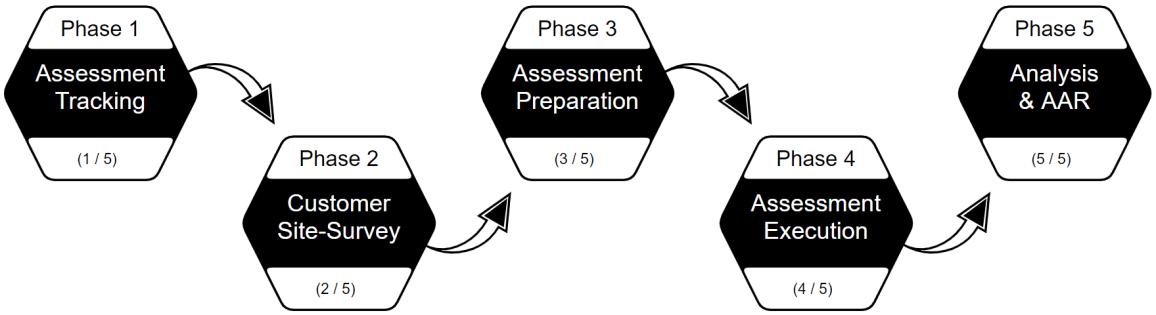


Figure 5. The Five Event Phases of CPT a Network Assessment

- **Future Operations Assessment Tracking**: The first event phase involves tracking, planning, and scheduling of customer organizations in the CPT's respective AOR. Cyber Planners, working closely alongside senior team leadership, coordinate with higher headquarters staff to properly space assessment timelines throughout a given year. An assessment enters the next event phase (Customer Site-Survey) approximately 90 days from the scheduled execution window. Team Leads and Mission Element Leads are normally selected before the next event phase milestone elapses.

- **Customer Site-Survey**: In the second phase, site-survey members, TL, MEL, Cyber Planner, and one to two operators, serving as technical advisors, travel to the customer's geographic area to establish contact with the Mission Owner and discuss assessment requirements. Factors in this discovery include but are not limited to identifying the number of networks to assess, classification level of each network, and type / number of devices residing on each network. Requirements gathered during this step are crucial and provide the foundation for all subsequent event phases.

- **Assessment Preparation**: Upon the return of the survey team, the Assessment Preparation event phase begins and is characterized by three main efforts: Mission Element staffing, tool testing and preparation, and administrative overhead as defined by the higher headquarters. Mission Element Operators are selected from the pool of available personnel based on surveyed requirements and individual qualification status. The ideal ME is staffed with an even mixture of experienced and inexperienced Operators in order to facilitate OJT and mentorship from the former to the latter. Once assembled, the ME then gathers and tests the requisite number of Deployable Mission Support System (DMSS) kits that will be used to perform on-site network collection during the fourth event phase (Assessment Execution). The Concept of Operations (CONOP) is concurrently drafted by CPT team leadership which codifies the operational aspects of each assessment as well as the relevant roles for each stakeholder in the assessment. A CONOP is ultimately signed by the higher headquarters commander, CPT OIC, and Mission Owner before each assessment execution can begin.

- **Assessment Execution**: Mission Elements depart for the assessment site to execute the fourth event phase once the team is prepared and CONOP has been signed. Operators systematically retest the DMSS kits upon

arrival to check for damaged or inoperable components. Pending gear status, the ME installs network hardware and begins the data collection process which typically last between two to four weeks. Once complete, the ME disconnects network hardware, returns home, and uploads the data to a lab environment where it is then analyzed for after-action reporting.

- **Analysis and After-Action Reporting**: The network assessment transitions to the final event phase begins when the ME returns home, unpacks the DMSS kits, and transfers collected data to the CPT lab environment for analysis. Team operators review the customer's data comparing the findings to the network's established baseline to uncover anomalies. The analysis is distilled into an After-Action Report (AAR) document which is distributed to CPT leadership and customer via the Mission Owner. The TL and MEL conclude the network assessment by collecting Lessons Learned (LL) from the Mission Element that can be used to improve future missions for the team.

3. The Structure: CPT Chain of Command and Operational Relationships

As military organizations, Cyber Protection Teams naturally operate in a highly rigid environment. A majority of network assessments conducted by CPTs are cyclic in nature and constitute one of the many DOD policy requirements for tenant organizations to remain active in the global digital enterprise. The supported and supporting relationships between a team's higher headquarters commander, and even the assessed customers, are bounded by the concept of authorities in Title 10 doctrine (i.e., applies to all services and not limited to one military branch). The relevant authorities in network assessments are listed below.

- **Operational Control** (OPCON): The functional authority of a commander to organize and employ military forces to accomplish an assigned task or objective. OPCON of a force can be associated with "getting the job done" but does not necessarily include the administrative,

logistical, or training support to execute a commander's intent (U.S. Army, 2016). The sample frame of CPTs in this research are operationally controlled by the Pacific Task Group Commander in the USINDOPACOM AOR.

- **Administrative Control** (ADCON): The functional authority of a commander to carry out the administrative support needed to sustain a military unit. Associated tasks with this authority can include the fulfillment of Manning, Training, and Equipping (MTE) requirements to maintain force readiness. Parent units who temporarily transfer OPCON to another commander will retain ADCON authority, a circumstance in which subordinate units maintain separate chains of command between operational and administrative support.

B. TACIT KNOWLEDGE PATHOLOGIES

With internal components of people, work, and structure defined, inputs returned from personnel within the sampled CPTs were analyzed to identify the flow and characteristics of tacit knowledge pathologies. A total of fourteen questionnaires were returned from five teams – four stationed in Oahu, Hawaii and one stationed in San Diego, California. With the support from two senior enlisted leaders from the sampled teams, three distinct paygrade groups anonymously contributed responses in support of the research effort. The ranges and categories of respondent paygrades are identified in Table 4.

Table 4. Questionnaire Respondent Paygrade Demographics

Respondent Paygrade Demographics		
Group Identifier	Paygrade Range	Group Size
Junior Enlisted Personnel	E-1 – E-6	8
Senior Enlisted Personnel	E-7 – E-9	5
Officer Personnel	O-1 – O-3	1
	Total:	14

Each of the nine questionnaire prompts were carefully developed to enhance our understanding of what kinds of tacit knowledge, or "know how" knowledge, manifested for the personnel involved in real-world operations. The responses from each member were digested in a two-part process to analyze emergent pathologies in the context of a CPT's congruence factors.

- **Initial respondent review**. All nine respondent questions were carefully analyzed and collated into one document for each team. Grouping data by team helped us identify trends that were generally consistent across a team to avoid individual outliers that could asymmetrically impact the behavior modeling process.

- **Congruence factor correlation**. A table was prepared with five column keys to contextualize the distilled input from team members. The first column was configured with a selectable dropdown field with five options to match the event phase of a network assessment. The second and third columns were labeled as "Actor" and "Recipient" respectively and configured with a second dropdown field containing "The People," "The Work," and "The Structure" options to reflect the bi-directional, cause and effect relationships of TCM internal components. A fourth column was labeled as "Source" and configured with a dropdown containing "Questionnaire," "JQR," and "Combination" options to identify where the source or sources of data were coming from. A fifth and final "Description" column captured free-form text to describe useful information concerning each row of the table. Figure 6—a custom image developed from our intermediate correlation table and wireframe flow-chart—captures the expanded dropdowns to show options that functioned as connective tissue between respondent answers and a particular pathology's anatomy. A total of seven individual pathologies emerged from our analysis across all five teams. The final results of the correlation can be seen in Table 5 along with an abbreviated description of each trend.

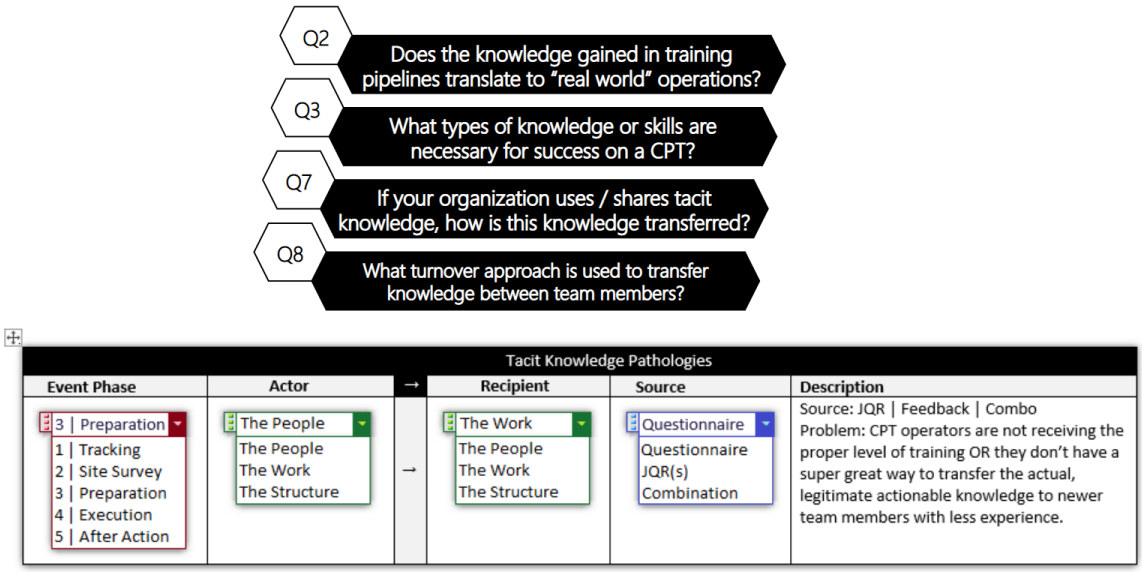


Figure 6. Correlation Table and Corresponding Questionnaire Questions

Table 5. Mapping Respondent Answers to TCM Components and Assessment Event Phases

Respondent Input / TCM Component / Event Phase Mapping					
#	Event Phase	Actor	→	Affected	Description
1	Phase 3: Preparation	People	→	Work	In some circumstances, qualified team members are not always available to sign line items in the JQR of newly onboarded members; members in this situation are often not fully prepared or qualified for their assigned CPT work role.
2	Phase 3: Preparation	Structure	→	People	Billeted operators do not always receive an equal or adequate level of pipeline training prior to onboarding **OR** operators do not have a reliable method or codified process to transfer actionable knowledge to newly onboarded members.
3	Phase 3: Preparation	Structure	→	Work	Much of an operator's "know-how" knowledge is gathered during on-site assessments; experienced operators are often the first choice for ME staffing, reducing exposure opportunities for less experienced team members to build tacit knowledge.
4	Phase 2: Site-Survey	People	→	Work	A lack of experience by the Site-Survey team members results in miscommunication and inaccurate assessment requirement development, hindering operator execution in later event phases.
5	Phase 3: Preparation	Structure	→	Work	There is no standardized method for accomplishing the event phases of a network assessment across the CPF; members who transfer from one CPT to another often find that their hard-earned, actionable knowledge is minimized and must readjust to a new team's workflow to regain lost execution efficiency.

Respondent Input / TCM Component / Event Phase Mapping					
#	Event Phase	Actor	→	Affected	Description
6	Phase 4: Execution	People	→	Work	Operators occasionally feel pressured to perform "rushed" assessments without the specialized / necessary tools; as a result, operators are not always able to hone analytical skills and often produce after-action reports with very little impact.
7	Phase 5: After-Action	Work	→	People	Some of the most valuable Lessons Learned (LL) stem from vulnerable or misconfigured networks; however, LL are sometimes written to reflect limited fault on the customer's behalf; valuable opportunities for individual / team tacit knowledge improvement are lost when messaging is prioritized over accurate LL.

C. BEHAVIOR MODELING

1. Model Design

Event modeling of the network assessment event phases was accomplished using the MP-Firebird tool, a web-based integrated development environment for Monterey Phoenix that supports syntax highlighting and code execution. MP's modeling paradigm is flexible enough to replicate a wide possibility of scenarios that occur in the physical world. In the case of real-world network assessments, two separate models were developed to capture the internal relationships between CPT components. Appendix A contains the readable MP source code for the baseline model and the combination of Appendices B and C (note the continuity of line numbering from Appendix B to Appendix C) contain the MP source code for the pathology model. Semantically, both models contain identical namespaces for root actors, event phases, precedence; however, our models deviate where actors exhibit behavioral differences as a result of additional Boolean characteristics. The remainder of this chapter refers to first model as the "baseline model" and second as the "pathology model." Six event grammar keywords and one language feature were used to replicate scope-complete permutations of network assessments.

- **`SCHEMA`**: A unique keyword used at the root (occurring first) of a MP source code file, serving as the parent object under which all subsequent event grammar belongs. The first and second model schemas were defined as **`Network_Assessment_Baseline`** and **`Network_Assessment_Pathology_Overlay`**, respectively.

- **`ROOT`**: Uniquely named keyword used to define the primary event components of a model. Each root declaration is used to group together characteristics that collectively describe its behavior in a **`SCHEMA`**'s model. Five event phases and four event actors were defined for both models addressed in this research.

- **`COORDINATE → DO`**: Keyword combination used for composition operations that "coordinate" behavior(s) between two or more root events. This operation was used to correlate the characteristics of each actor to key points across relevant event phases.

- **`IF → THEN → DO`**: Keyword combination used to test branching behavior as a result of conditional logic. These keywords were extensively used in the second model to test the result of an actor's Boolean characteristics.

- **`REPORT → CLEAR → SAY → SHOW`**: Keyword combination used to visually display pathology match statistics for a given test by defining a unique report name (**`REPORT`**), clearing any polluted statistics from a variable (**`CLEAR`**), formatting a message's contents (**`SAY`**), then printing a message (**`SHOW`**) in the IDE's graphed output.

- **`/* Code Block Comment */`**: Human readable, non-executable feature of the Monterey Phoenix language that begins with a leading **`/*`** and ends with a trailing **`*/`**. Referred to as "commenting" or "commenting out" in this research, these characters are used in the IDE's code editor to either (1) record in-line documentation for a block of code or (2) stop a block of code from executing at runtime as a means to control model behavior.

The baseline model reflected the ideal state of CPT components in which team members are fully qualified and event phases are unconditionally completed. Assessment actors were defined with static, non-branching characteristics such as "**`Training_complete`**" and "**`Familiar_with_workflow`**" that intentionally abstracted away adverse team performance. Beyond event phases and actors, the first

model established a baseline representation network assessment, using only four `COORDINATE` statements to set event phase precedence. (e.g., the Site-Survey event phase precedes the Assessment Preparation event phase). Execution of the first model at a scope level of `1` without additional relationships or opportunities for branch behavior resulted in exactly one trace result.

2. Pathology Analysis

The second model extended the baseline with conditional logic to reflect the distilled answers from questionnaire respondents. Specifically, the pathology model differed from the baseline model in two important ways:

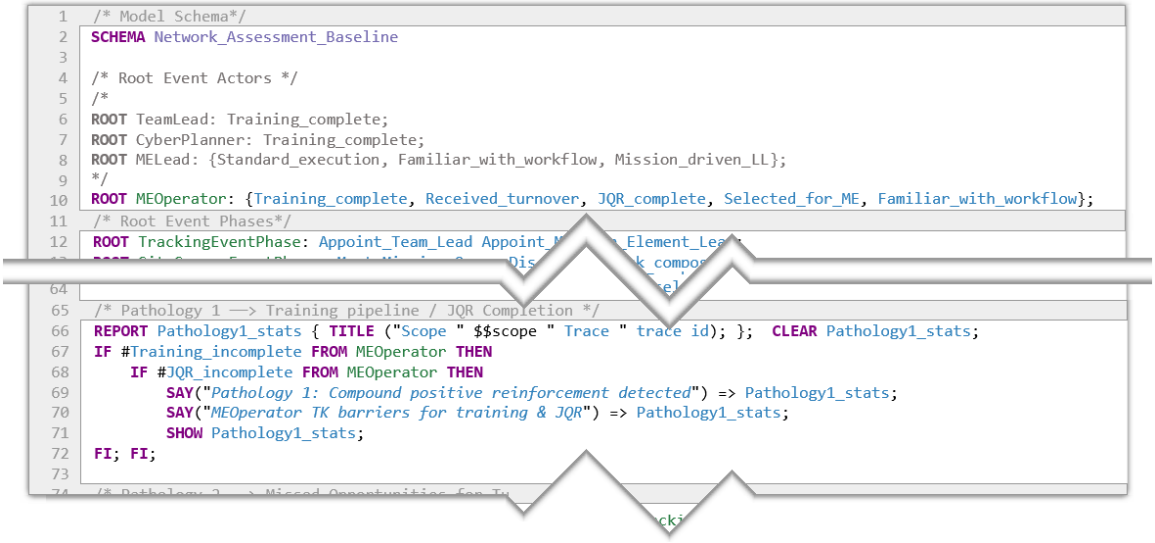
1. Behaviors for each event phase actor were converted from static fields to Boolean case values. These changes created realistic scenarios in which tacit knowledge barriers hinge on a team member's personal attributes or the attributes of others. For example, Mission Element Operators who encounter issues with training or JQR completion may have divergent outcomes from peers who do not encounter these barriers at all.

2 Additional `COORDINATE` statements were added to associate the Boolean conditions of event actors to strategic points in the network assessment process. These conditional relationships recreate the experiences of CPT personnel represented in questionnaire responses.

Seven unique pathologies—captured in Table 6—were constructed to test the outcome of added Boolean behavior characteristics and coordinated relationships. Unmodified execution of the pathology model—i.e., without excluding event actors from specific pathology tests via code comment blocks—resulted in 512 unique traces—reflecting a high degree of potential variance throughout an assessment. Code block comments were used to temporarily exclude event actors from tests who did not have characteristics that affected a given pathology's logic at runtime. Figure 7 captures an example of these comments around the `TeamLead`, `CyberPlanner`, and `MELead` event actors to exclude the root events from the Pathology 1 logic test starting on line 66.

Table 6. Table of Constructed Pathologies

Table of Constructed Pathologies		
Name	Event Actor(s)	Event Phase
Pathology 1	Mission Element Operators	4 | Assessment Execution
Pathology 2	Mission Element Operators	3 | Assessment Preparation
Pathology 3	Team Lead Mission Element Operators	3 | Assessment Preparation
Pathology 4	Team Lead Cyber Planner	2 | Site-Survey
Pathology 5	Mission Element Lead Mission Element Operators	3 | Assessment Preparation
Pathology 6	Mission Element Lead	4 | Assessment Execution
Pathology 7	Mission Element Lead	5 | Analysis and AAR



```
/* Model Schema*/
SCHEMA Network_Assessment_Baseline

/* Root Event Actors */
/*
ROOT TeamLead: Training_complete;
ROOT CyberPlanner: Training_complete;
ROOT MELead: {Standard_execution, Familiar_with_workflow, Mission_driven_LL};
*/
ROOT MEOperator: {Training_complete, Received_turnover, JQR_complete, Selected_for_ME, Familiar_with_workflow};
/* Root Event Phases*/
ROOT TrackingEventPhase: Appoint_Team_Lead Appoint_
                                                    Element_Lea
                                                    k compos
                                                    el
/* Pathology 1 --> Training pipeline / JQR Completion */
REPORT Pathology1_stats { TITLE ("Scope " $$scope " Trace " trace id); };  CLEAR Pathology1_stats;
IF #Training_incomplete FROM MEOperator THEN
    IF #JQR_incomplete FROM MEOperator THEN
        SAY("Pathology 1: Compound positive reinforcement detected") => Pathology1_stats;
        SAY("MEOperator TK barriers for training & JQR") => Pathology1_stats;
        SHOW Pathology1_stats;
FI; FI;
```

Figure 7. Excluding Event Actors with Code Comment Characters.

Analysis for each of the seven pathologies is listed below and reflected in Figures 8 through 14. Each pathology's associated number corresponds to the same numbers shown previously in Table 5. The scope for each pathology was set to a value of `1` to limit trace

output complexity between event phases and actors. Trace results from each pathology were analyzed for the presence of positive reinforcement which, if uncorrected, could indicate negative or unwanted inefficiencies in the network assessment process.

Table 7. Pathology Model Execution Results

Model Execution Results			
Root Event Actors	ROOT Name	Traces	Events
Team Lead	`TeamLeaad`	2	4
Cyber Planner	`CyberPlannner`	2	4
Mission Element Lead	`MELead`	8	32
Mission Element Operator	`MEOperator`	32	192
	Event Actor Totals	44	232

Root Event Phases	ROOT Name	Traces	Events
Assessment Tracking	`TrackingEventPhase`	1	3
Site-Survey	`SiteSurveyEventPhaase`	5	18
Assessment Preparation	`PreparationEventPhase`	1	6
Assessment Execution	`ExecutionEventPhase`	1	4
Analysis & After-Action Reporting	`AnalysisAAREventPhase`	1	5
	Event Phase Totals	9	36

Pathology 1 | Training pipeline and JQR Completion

- Event actor: Mission Element Operators
- Event Phase: Assessment Execution
- Summary & Analysis: An ME Operator encounters barrier(s) to Tacit Knowledge (TK) development when he or she has not had the opportunity to complete the codified training pipeline and when senior team members are not available / cannot support JQR completion. Model execution with only the ME Operator enabled resulted in 32 unique traces with five traces (15.6%) exhibiting compound TK barriers. Nested logic successfully

captured possible scenarios where both training and qualification status inefficiencies could impact an operator's ability for team contribution via tacit knowledge.

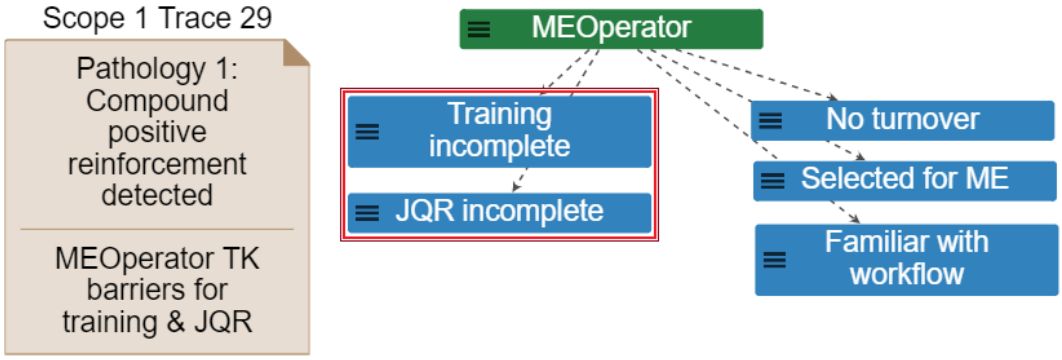


Figure 8. Pathology 1 Trace Result

Pathology 2 | Unstructured Opportunities for Turnover

- Event Actor: Mission Element Operators
- Event Phase: Assessment Preparation
- Summary & Analysis: Tacit knowledge barriers develop for CPT personnel when departing and arriving members encounter unstructured opportunities for turnover, lengthening the amount of time required to become fully integrated into team workflows. While this barrier is not limited to one work role, the ME Operator was used to represent CPT personnel as a whole and could easily be exchanged with another role. Two separate logic tests (2a and 2b) were developed to detect scenarios in which arriving members do not have the opportunity to conduct turnover and (2a) have not completed the training pipeline or (2b) have not yet completed the work role JQR. Model execution with only the ME Operator enabled resulted in 32 unique traces exhibiting TK barriers in pathology 2a with four traces (12.5%), pathology 2b with four traces (12.5%), and presence of both pathologies with four traces (12.5%). The

benefit of scope-complete modeling is evident in this result, capturing both cases as well as overlap where unmitigated barriers in training / qualification (TCM: structure) are compounded with barriers in turnover (TCM: people).

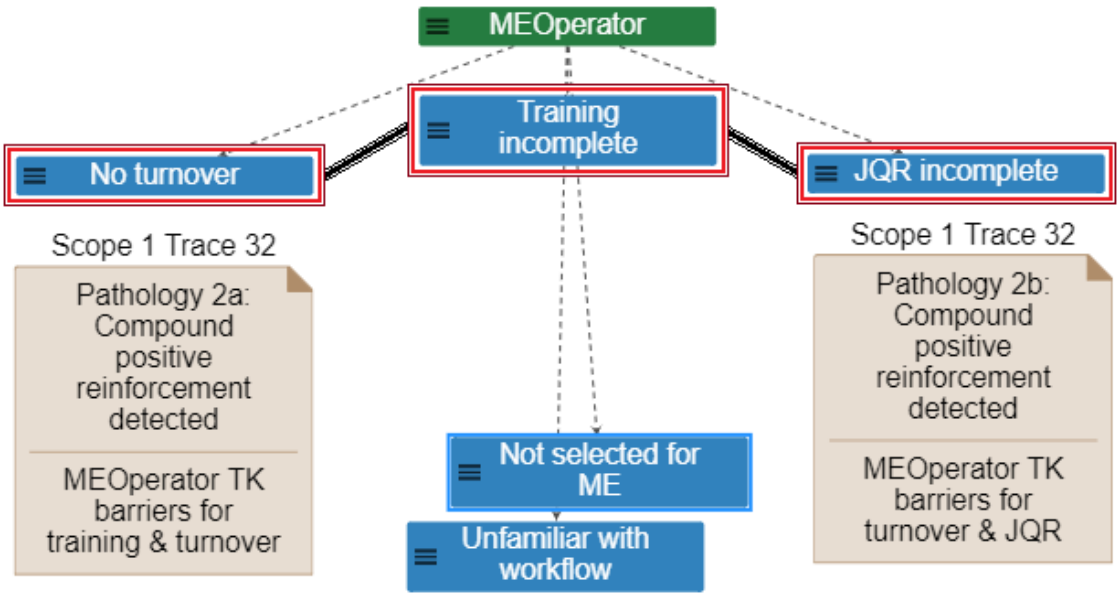


Figure 9. Pathology 2 Trace Result

Pathology 3 | Unbalanced Mission Element Staffing

- Event Actors: Team Lead, Mission Element Operator
- Event Phase: Assessment Preparation
- Summary & Analysis: Questionnaire respondents identified hands-on training during assessment event phases as one of the most valuable resources for tacit knowledge development on a CPT. As a result, Operators encounter tacit knowledge barriers when not selected for Mission Element staffing in the preparation event phase. Model execution with only the TL (staff selector) and ME Operator (potential staff selectee) enabled resulted in 64 unique event traces with five traces (7.8%) matching pathology 3 conditions. Interestingly, the addition of a Team

Lead effectively doubled the trace count (possible permutations) while concurrently reducing instances of positive reinforcement. Figure 10 captures this scenario in which no relationship exists between the Team Lead, appointed during the first event phase, and Operator who is not selected for the ME in the third event phase. Analysis revealed an unexpected causal relationship between the first, second, and third pathologies in which barriers to tacit knowledge are compounded when issues occur in two or more consecutive event phases.

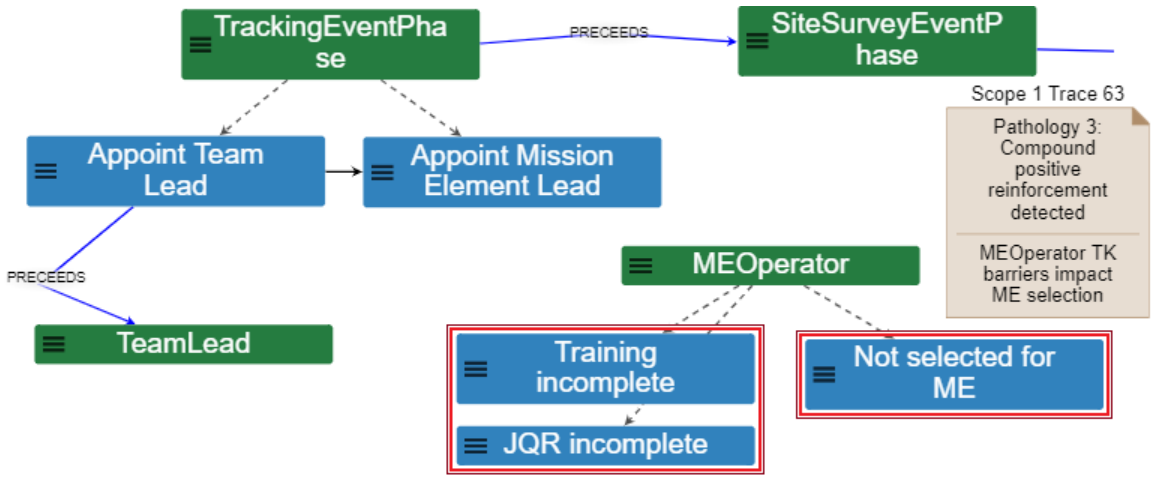


Figure 10. Pathology 3 Trace Result

Pathology 4 | Site-Survey Team Experience

- Event Actors: Team Lead, Cyber Planner
- Event Phase: Site-Survey
- Summary & Analysis: Site-Surveys are integral to the assessment process as subsequent event phases cascade from requirements identified in this step. Team Leads and Cyber Planners who encounter tacit knowledge barriers during a survey, be it administrative experience or technical proficiency, impact Mission Elements in the third, fourth, and fifth event phases. Logic was written to identify branch scenarios where limited

experience for both actors were present. Model execution with only the TL and Cyber Planner roles enabled resulted in four unique traces with one trace (25%) exhibiting a TK barrier. Although positive reinforcement only appeared once, the influence of surveys on other event phases cannot be ignored.

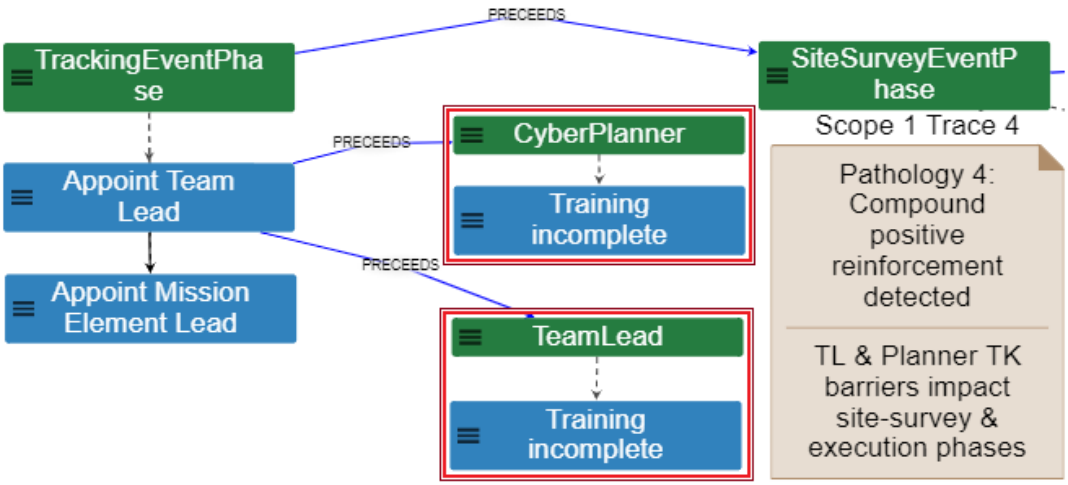


Figure 11. Pathology 4 Trace Result

Pathology 5 | Inter-CPT Workflow Continuity

- Event Actors: Mission Element Lead, Mission Element Operator
- Event Phase: Assessment Preparation
- Summary & Analysis: Unstructured assessment patterns across the CPF introduce tacit knowledge barriers when team members depart from one CPT and arrive at another, only to find unfamiliar workflows that inhibit efficiency. Model execution with only the MEL and ME Operator enabled resulted in 128 unique traces with 32 traces (25%) exhibiting TK barriers. As heavy lifters in the assessment process, ME Leads and ME Operators exhibit characteristics that interface with several event phases. Figure 12 captures tasks associated with preparation that require unfamiliar members

to focus on task semantics before actionable knowledge can be reconstituted.

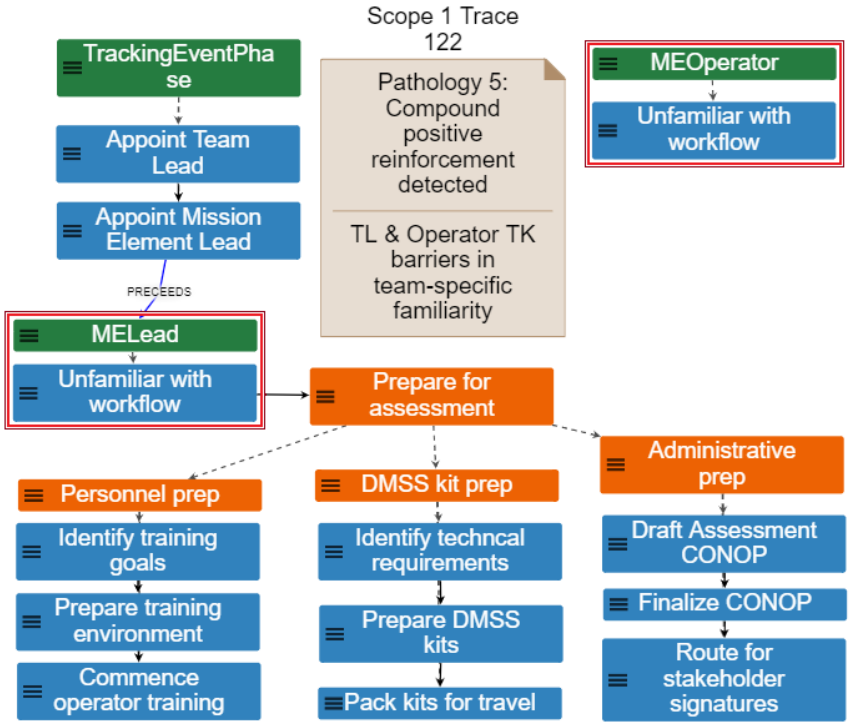


Figure 12. Pathology 5 Trace Result

Pathology 6 | Accelerated Assessment Execution

- Event Actors: Mission Element Lead
- Event Phases: Assessment Execution
- Summary & Analysis: As the senior team member and appointed supervisor, Mission Element Leads travel with operators to the customer site and oversee data collection that feeds after-action reporting. In some cases, operational factors require a compressed execution window which in turn causes the ME Lead to modify the actionable tasks for his or her team. Test logic for this pathology was developed with the intent to capture heuristic patterns that develop into tacit knowledge barriers over a

period of time. Model execution with only the MEL enabled resulted in four traces (50%) exhibiting TK barriers. Although MEs *do* encounter compressed windows, the number of traces exhibiting positive reinforcement are artificially high when compared to questionnaire respondent answers.

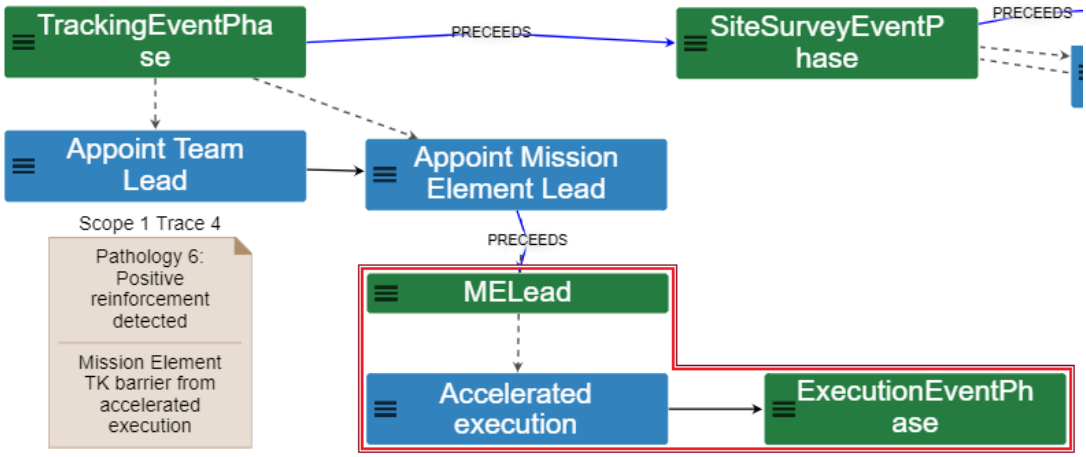


Figure 13. Pathology 6 Trace Result

- **Pathology 7** | Input Sources for Lessons Learned
  - Event Actor: Mission Element Leads
  - Event Phase: Analysis and After-Action Reporting
  - Summary & Analysis: The development of lessons learned following an operation act as a feedback loop, identifying areas for improvement in both preparation and execution phases. In some cases, lessons learned are framed in a way that insulates a customer from the results of its own assessment. Mission Elements that encounter this form of tacit knowledge barrier develop heuristic trends over time and cannot fully capitalize on the opportunities to improve actionable knowledge. Model execution with only the MEL enabled resulted in four traces (50%) exhibiting TK

barriers. As with pathology 6, this level of positive reinforcement is artificially high when compared to respondent answers.

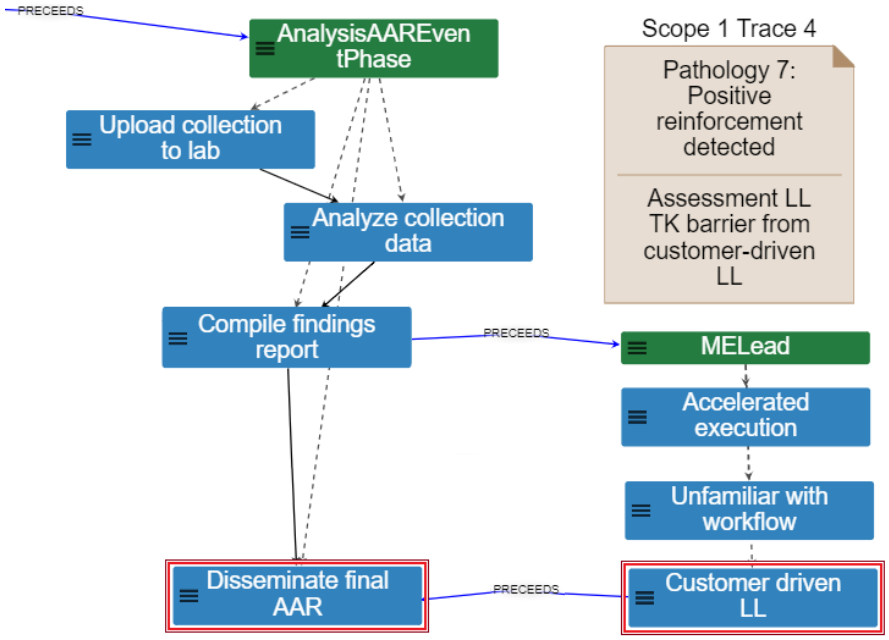


Figure 14. Pathology 7 Trace Result

D. SUMMARY

Figure 15 visually represents the seven tacit knowledge pathologies that overlay CPT network assessments. Each event phase has been color coded and linked to its associated knowledge flow. Individual pathologies are displayed as boxes with the acting component, affected component, and direction of affect flow. Numbers for each pathology in the figure correspond to respondent answers in Table 5 listed previously. The forward arrows (blue / green / yellow arrows originating left and flowing right) represent the presence of tacit knowledge barriers that affect CPT congruence within the life cycle one network assessment. The reverse arrows (red / purple arrows originating right and flowing left) represent barriers that heuristically affect CPT congruence over the span of multiple assessments.

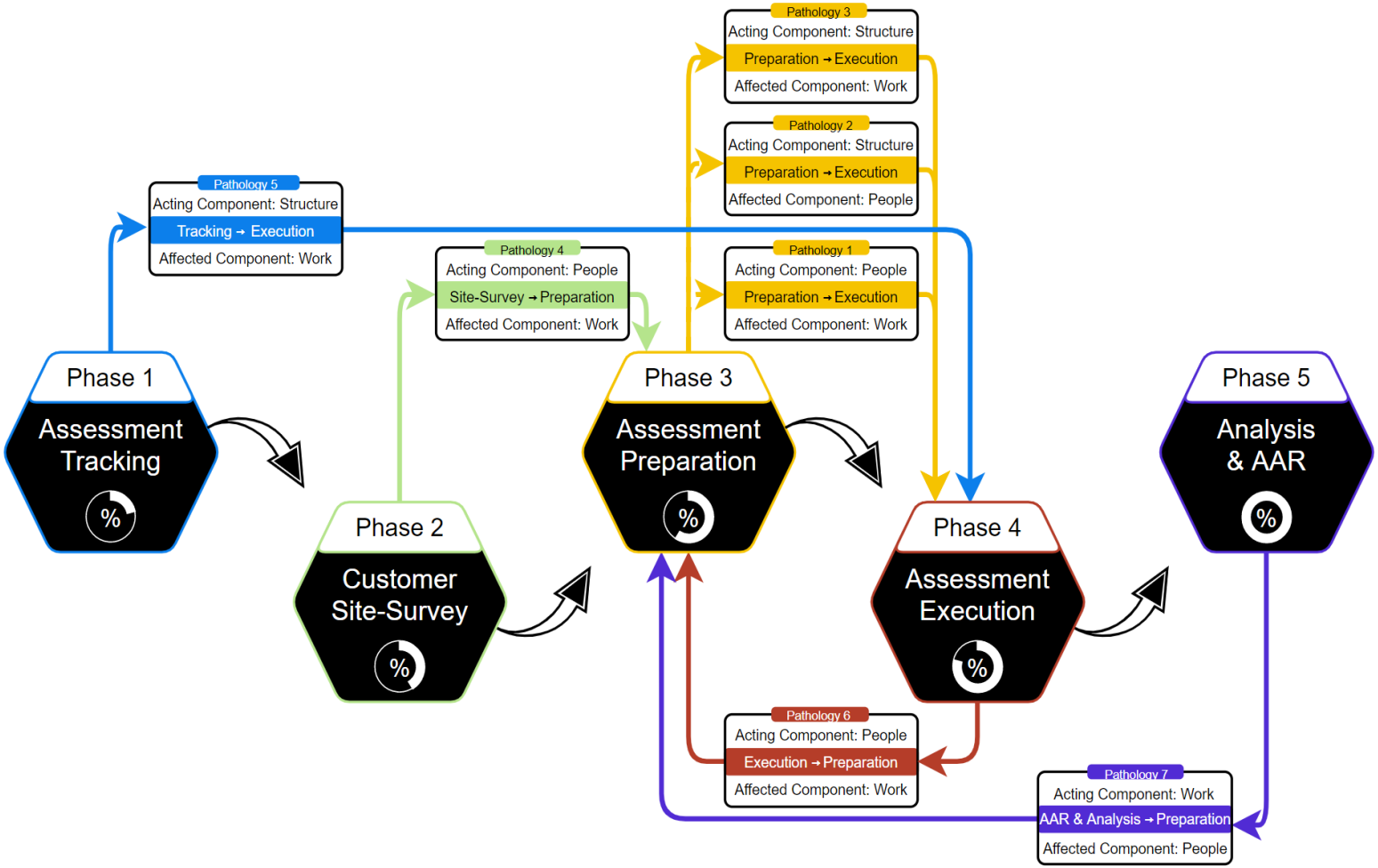


Figure 15. Network Assessment Event Phases and Tacit Knowledge Pathology Overlay

To answer the first research question—how does the inclusion of tacit knowledge into The Congruence Model impact the model's determination of organizational fit and performance?— the inclusion of tacit knowledge as factor for congruence exposes unique, intra-component pathologies that could have been overlooked were people, work, and structure the only factors to be analyzed. Moreover, the use of quantitative modeling via Monterey Phoenix highlighted several cases where the presence of two or more barriers produced compound positive reinforcement for multiple team members across two or more event phases.

To answer the second research question—how can tacit knowledge be measured within the Cyber Protection Teams as a method to test its inclusion into The Congruence Model?—applying a combination of qualitative data collection (CPT personnel questionnaires) and quantitative analysis (trace results from Monterey Phoenix model execution) proved to be an effective way to test for the presence and impact of tacit knowledge barriers that inhibit organization efficiency. The expressive MP event grammar was easily mapped to CPT-specific components and produced event traces that could be interpreted to improve current and future workflows.

V. CONCLUSION

This chapter concludes the body of research with a presentation of recommendations, study limitations, and promising areas for future research. As addressed in Chapter II, the actionable nature of tacit knowledge makes it an extremely valuable component of any organization. This is equally true regarding the teams that compile the Cyber Protection Force who rely on cyberspace workforce professionals to execute defensive mission across the globe. The characteristics that make tacit knowledge (a resource internalized by each person of a team to accomplish complex tasks with intangible context) valuable also make it difficult to codify, capture, and maintain with high rates of personnel turnover. The results captured in this work present the value of actionable knowledge not just for the CPF, but for organizations across the Title 10 Cyber Mission Force enterprise.

A. RECOMMENDATIONS

1. Congruence Analysis Using All Components of TCM

The work accomplished in this research—combining The Congruence Model with Monterey Phoenix to enable programmatic, scope-complete behavior modeling—is a positive move toward a better understanding of not only knowledge, but how knowledge affects the U.S. military's cybersecurity workforce. Future research in this area should strive to use all four core factors of TCM to determine organization congruence and / or behavior modeling.

2. Monterey Phoenix Behavior Modeling

The executable event grammar found in Monterey Phoenix is extremely flexible and should be considered for future bodies of research that include event and / or behavior modeling. Several data points in our research came directly from real-world operators with first-hand experience about the network assessment process from five separate organization perspectives. Qualitative collection from our sample frame produced positive *and* negative data points, both of which were instrumental in our search for tacit knowledge

pathologies. This flexible event grammar is displayed in Figure 16 which visualizes the Boolean characteristics for Mission Element Operators and corresponding test for members who have completed training pipelines / qualification requirements (negative reinforcement) and those who have not (positive reinforcement).

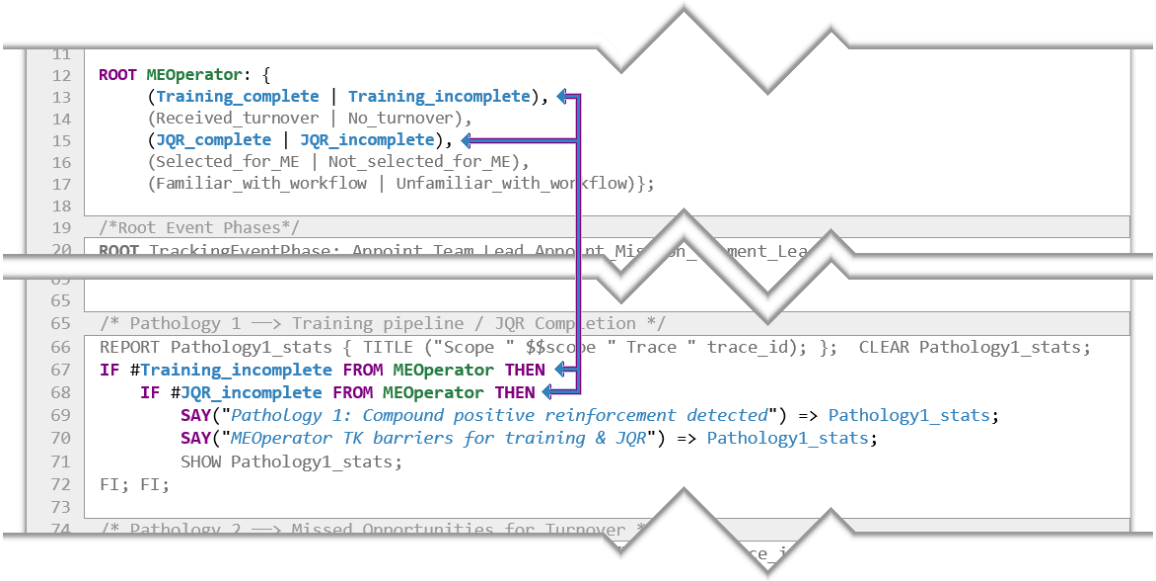


Figure 16. ME Operator Characteristics and Corresponding Pathology

3. Measurable Value Mapping.

Research involving behavioral modeling and analysis—using Monterey Phoenix or equivalent platform—should develop methods to apply weighted values for wanted and unwanted outcomes. Using the assessment execution event phase as an example, binary yes / no branches are a valid way to introduce scenarios where a Mission Element is missing one network cable vice an entire DMSS kit; however, these are not circumstances with equal impact. Network cables can easily be replaced whereas each DMSS kit is an integral part of the assessment process. Model relationships should be configured to expose pathology logic that reflects realistic, real-world cause and affect scenarios.

4. Cyber Mission Force Application

The approach used in this research to model operational aspects of the CPF should be adapted and applied to other team and communities in the Cyber Mission Force. Beyond tacit knowledge pathologies, team input and relational modeling proved to be an effective process for identifying, building, and executing scope-complete models that reflected realistic operational scenarios. Figure 17 visualizes the notable discovery of tacit knowledge barriers in accelerated assessment timelines and AAR lessons learned development of that heuristically affect tacit knowledge and team congruence over the course of several network assessments. Operational units across the CMF – Joint Force Headquarters-Cyber units, tactically-focused offensive Cyber Mission Teams and National Mission Teams, and corresponding support teams – can use the approach trailblazed in this research to discover and mitigate challenges that may not be readily visible in day-to-day operations.

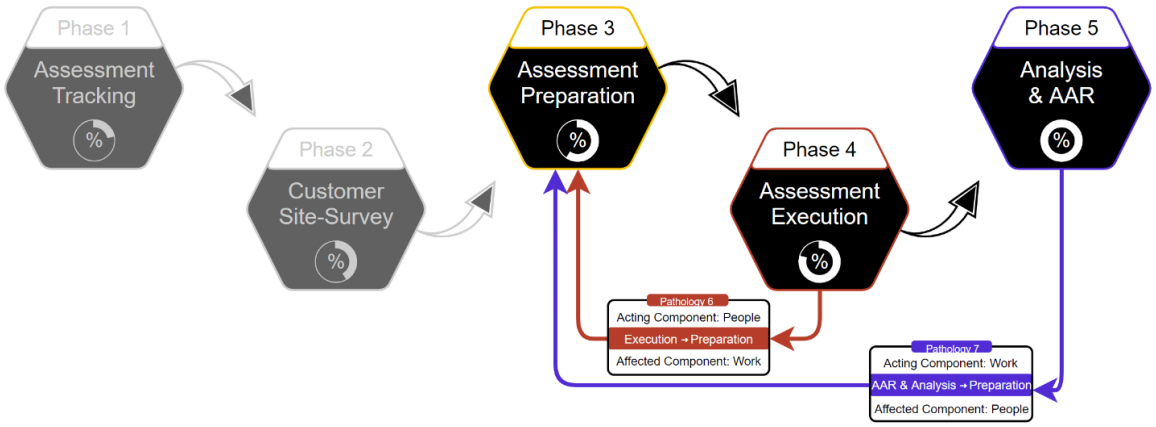


Figure 17. Phases 3 through 5

B. LIMITATIONS

This study was a focused application of The Congruence Model to discover and subsequently measure tacit knowledge pathologies in the network assessment process of Cyber Protection Teams. Although this research was guided by thorough planning and diligent execution, some issues did arise that affected our work. The points listed below

capture our own lessons learned and should be taken into consideration for future research efforts.

1. We anticipated the restrictions of face-to-face interviews and government travel limitations due to the ongoing COVID-19 pandemic. These restrictions on physical contact during the questionnaire process and the original intent to hold in-person focus groups affected our ability to gather first-hand data collection in the day-to-day operations and training cycles of the teams

2. There is no assembled collection of literature that addresses either tacit knowledge or tacit knowledge management regarding CPTs or any Cyber Mission Force component for that matter. Although anticipated, this presented significant hurtles during the initial research and experimentation development phases.

3. Although the USINDOPACOM AOR includes a significant portion of the U.S. military's cybersecurity workforce, we did not receive the expected number and diversity of team participants from the junior enlisted and officer demographics. Ultimately, three limiting factors affected survey participation:

    - Geographic and temporal separation between the research team and pool of participants.
    - CDC guidance, Restriction of Movement (ROM), and vaccine availability regarding the Corona Virus Pandemic.
    - Limited personnel actively supporting high operation tempos to comply with social distancing and work-from-home guidance.

5. Stated in Chapter I, tacit knowledge is difficult to capture; especially in the context of a comprehensive knowledge management framework. Although questionnaire participation represented a significant portion of our data points, the environment in which tacit knowledge exists—the

minds and actions of individual people—means we were unable to capture the full spectrum of solutions used by personnel to operate around the presence compound tacit knowledge barriers.

6. While the event grammar of Monterey Phoenix is much easier to learn than a feature-rich language like C or Java, we encountered an unexpected learning curve with some of the language's semantics and platform execution. Specifically, root actors with binary values, such as `JQR_complete` or `JQR_incomplete`, each doubled the number of resulting traces. In some cases, the diligent use of `COORDINATE` statements was needed to construct the necessary relationships between event phases and event actors.

C. FUTURE STUDIES

This study only covered tacit knowledge modeling within the Cyber Protection Teams, but the structure and methods described used can easily be expanded for future research opportunities. Some considerations for future research areas are:

- Similar study using other areas of the Cyber Mission Force

(1) Offensive Cyber Teams

(2) Other Defensive Cyber Teams

- Similar study to compare tacit knowledge pathologies between military service branches

(1) E.g., explore the differences and approaches to tacit knowledge management between U.S. Army, Marine Corps, Navy, Air Force, Coast Guard, and Space Force.

- An updated study in the next three to five years to compare and contrast how cyberspace workforce communities manage tacit knowledge over time.

(1) In the anecdotal experience of the research team, CMF teams are constantly in a state of churn to advance tactics, teamwork, and operations. A comparison between future findings and those addressed in this report may reveal interesting trends that could lead to better methods for workforce adaption.

D. CONCLUSION

Tacit knowledge has been identified a core factor that needs to be addressed within the Cyber Protection Force. Is it possible to measure and include this resource as an additional component in The Congruence Model? Yes, captured and analyzed in Chapter IV. The recommendations stated in this chapter include prescriptions for knowledge management that support CPT operations. Failing to do so may result in lost efficiency in both personnel training and mission effectiveness. At the individual team level, members and team leaders can implement models of stewardship discussed in this research that improve the effectiveness for all network assessment event phases. At the theater level, CPF leadership and operational commanders can review the Chapter IV findings to improve tacit knowledge workflows for intra-team cohesiveness, training, and communication.

APPENDIX A. MONTEREY PHOENIX NETWORK ASSESSMENT BASELINE MODEL

```
/* Model Schema*/
SCHEMA Network_Assessment_Baseline

/* Root Event Actors */
ROOT TeamLead: Training_complete;
ROOT CyberPlanner: Training_complete;
ROOT MELead: {Standard_execution, Familiar_with_workflow, Mission_driven_LL};
ROOT MEOperator: {Training_complete, Received_turnover, JQR_complete, Selected_for_ME, Familiar_with_workflow};


/* Root Event Phases*/
ROOT TrackingEventPhase: Appoint_Team_Lead Appoint_Mission_Element_Lead;
ROOT SiteSurveyEventPhase: Meet_Mission_Owner Discuss_network_composition;
ROOT PreparationEventPhase:
     Review_survey_results ME_Operator_selection Prepare_for_assessment;
     Prepare_for_assessment: {Personnel_prep, DMSS_kit_prep, Administrative_prep};
     Personnel_prep: (Identify_training_goals Prepare_training_environment Commence_operator_training);
     DMSS_kit_prep: (Identify_techncal_requirements Prepare_DMSS_kits Pack_kits_for_travel);
     Administrative_prep: (Draft_Assessment_CONOP Finalize_CONOP Route_for_stakeholder_signatures);
ROOT ExecutionEventPhase: Deploy_assessment_gear Collection_completes Return_home;
ROOT AnalysisAAREventPhase: Upload_collection_to_lab Analyze_collection_data
                            Compile_findings_report Disseminate_final_AAR;


/* Event Phase Coordination & Precedence */
COORDINATE $a: TrackingEventPhase, $b: SiteSurveyEventPhase
     DO ADD $a PRECEEDS $b; OD;

COORDINATE $a: SiteSurveyEventPhase, $b: PreparationEventPhase
     DO ADD $a PRECEEDS $b; OD;

COORDINATE $a: PreparationEventPhase, $b: ExecutionEventPhase
     DO ADD $a PRECEEDS $b; OD;

COORDINATE $a: ExecutionEventPhase, $b: AnalysisAAREventPhase
     DO ADD $a PRECEEDS $b; OD;
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. MONTEREY PHOENIX NETWORK ASSESSMENT PATHOLOGY OVERLAY (1 / 2)

```
/* Model Schema*/
SCHEMA Network_Assessment_Pathology_Overlay

/* ROOT Event Actors */
ROOT TeamLead: (Training_complete | Training_incomplete);
ROOT CyberPlanner: (Training_complete | Training_incomplete);
ROOT MELead: {
     (Standard_execution | Accelerated_execution),
     (Familiar_with_workflow | Unfamiliar_with_workflow),
     (Mission_driven_LL | Customer_driven_LL)};
ROOT MEOperator: {
     (Training_complete | Training_incomplete),
     (Received_turnover | No_turnover),
     (JQR_complete | JQR_incomplete),
     (Selected_for_ME | Not_selected_for_ME),
     (Familiar_with_workflow | Unfamiliar_with_workflow)};

/*Root Event Phases*/
ROOT TrackingEventPhase: Appoint_Team_Lead Appoint_Mission_Element_Lead;
ROOT SiteSurveyEventPhase: Meet_Mission_Owner Discuss_network_composition;
ROOT PreparationEventPhase: Review_survey_results ME_Operator_selection Prepare_for_assessment
     Prepare_for_assessment: {Personnel_prep, DMSS_kit_prep, Administrative_prep};
     Personnel_prep: (Identify_training_goals Prepare_training_environment Commence_operator_training);
     DMSS_kit_prep: (Identify_techncal_requirements Prepare_DMSS_kits Pack_kits_for_travel);
     Administrative_prep: (Draft_Assessment_CONOP Finalize_CONOP Route_for_stakeholder_signatures);
ROOT ExecutionEventPhase: Deploy_assessment_gear Collection_completes Return_home;
ROOT AnalysisAAREventPhase: Upload_collection_to_lab Analyze_collection_data
                            Compile_findings_report Disseminate_final_AAR;

/* Event Phase Coordination & Precedence */
COORDINATE $a: TrackingEventPhase, $b: SiteSurveyEventPhase
           DO ADD $a PRECEEDS $b; OD;

COORDINATE $a: SiteSurveyEventPhase, $b: PreparationEventPhase
           DO ADD $a PRECEEDS $b; OD;

COORDINATE $a: PreparationEventPhase, $b: ExecutionEventPhase
           DO ADD $a PRECEEDS $b; OD;

COORDINATE $a: ExecutionEventPhase, $b: AnalysisAAREventPhase
           DO ADD $a PRECEEDS $b; OD;

/* Event Actor Coordination & Precedence */
COORDINATE $a: Appoint_Team_Lead FROM TrackingEventPhase,
           $b: TeamLead
           DO ADD $a PRECEEDS $b; OD;

COORDINATE $a: Appoint_Mission_Element_Lead FROM TrackingEventPhase,
           $b: MELead
           DO ADD $a PRECEEDS $b; OD;

COORDINATE $a: Unfamiliar_with_workflow FROM MELead,
           $b: Prepare_for_assessment FROM PreparationEventPhase
           DO ADD $a PRECEEDS $b; OD;

COORDINATE $a: TeamLead,
           $b: MELead,
           $c: Compile_findings_report FROM AnalysisAAREventPhase
           DO ADD $a PRECEDES $c, $b PRECEDES $c; OD;
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. MONTEREY PHOENIX NETWORK ASSESSMENT PATHOLOGY OVERLAY (2 / 2)

```
/* Pathology 1 —> Training pipeline / JQR Completion */
REPORT Pathology1_stats { TITLE ("Scope " $$scope " Trace " trace_id); };  CLEAR Pathology1_stats;
IF #Training_incomplete FROM MEOperator THEN
    IF #JQR_incomplete FROM MEOperator THEN
        SAY("Pathology 1: Compound positive reinforcement detected") => Pathology1_stats;
        SAY("MEOperator TK barriers for training & JQR") => Pathology1_stats;
        SHOW Pathology1_stats;
FI; FI;
/* Pathology 2 —> Missed Opportunities for Turnover */
REPORT Pathology2a_stats { TITLE ("Scope " $$scope " Trace " trace_id); };  CLEAR Pathology2a_stats;
IF #Training_incomplete FROM MEOperator THEN
    IF #No_turnover FROM MEOperator THEN
        SAY("Pathology 2a: Compound positive reinforcement detected") => Pathology2a_stats;
        SAY("MEOperator TK barriers for training & turnover") => Pathology2a_stats;
        SHOW Pathology2a_stats; FI; FI;
REPORT Pathology2b_stats { TITLE ("Scope " $$scope " Trace " trace_id); };  CLEAR Pathology2b_stats;
IF #No_turnover FROM MEOperator THEN
    IF #JQR_incomplete FROM MEOperator THEN
        SAY("Pathology 2b: Compound positive reinforcement detected") => Pathology2b_stats;
        SAY("MEOperator TK barriers for turnover & JQR") => Pathology2b_stats;
        SHOW Pathology2b_stats;
FI; FI;
/* Pathology 3 —> ME Staffing & Experience Issue */
REPORT Pathology3_stats { TITLE ("Scope " $$scope " Trace " trace_id); };  CLEAR Pathology3_stats;
IF #Training_incomplete FROM MEOperator THEN
    IF #JQR_incomplete FROM MEOperator THEN
        IF #Not_selected_for_ME FROM MEOperator THEN
           SAY("Pathology 3: Compound positive reinforcement detected") => Pathology3_stats;
           SAY("MEOperator TK barriers impact ME selection") => Pathology3_stats;
           SHOW Pathology3_stats;
FI; FI; FI;
/* Pathology 4 —> Survey Team Lacks Experience  */
REPORT Pathology4_stats { TITLE ("Scope " $$scope " Trace " trace_id); };  CLEAR Pathology4_stats;
IF #Training_incomplete FROM TeamLead THEN
    IF #Training_incomplete FROM CyberPlanner THEN
        SAY("Pathology 4: Compound positive reinforcement detected") => Pathology4_stats;
        SAY("TL & Planner TK barriers impact survey/ execution phase") => Pathology4_stats;
        SHOW Pathology4_stats;
FI; FI;
/* Pathology 5 —> No Cross-CPT Workflow Continuity */
REPORT Pathology5_stats { TITLE ("Scope " $$scope " Trace " trace_id); };  CLEAR Pathology5_stats;
IF #Unfamiliar_with_workflow FROM MELead THEN
    IF #Selected_for_ME FROM MEOperator THEN
        IF #Unfamiliar_with_workflow FROM MEOperator THEN
            SAY("Pathology 5: Compound positive reinforcement detected") => Pathology5_stats;
            SAY("TL & Operator TK barriers in team familiarity") => Pathology5_stats;
            SHOW Pathology5_stats;
FI; FI; FI;
/* Pathology 6 —> Accelerated Assessment Barriers */
REPORT Pathology6_stats { TITLE ("Scope " $$scope " Trace " trace_id); };  CLEAR Pathology6_stats;
IF #Accelerated_execution FROM MELead THEN
   SAY("Pathology 6: Positive reinforcement detected") => Pathology6_stats;
   SAY("Mission Element TK barrier from accelerated execution") => Pathology6_stats;
   SHOW Pathology6_stats;
FI;
/* Pathology 7 —> Lessons Learned Barriers */
REPORT Pathology7_stats { TITLE ("Scope " $$scope " Trace " trace_id); };  CLEAR Pathology7_stats;
IF #Customer_driven_LL FROM MELead THEN
    SAY("Pathology 7: Positive reinforcement detected") => Pathology7_stats;
    SAY("Assessment LL TK barrier from customer-driven LL") => Pathology7_stats;
    SHOW Pathology7_stats;
FI;
```

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Auguston, Mikhail. (2015). *Use Monterey Phoenix (MP) to reason about behaviors of your system. Using your knowledge. In your words.* (Version 4) [Web-Based App] https://wiki.nps.edu/display/MP/Monterey+Phoenix+Home

Ambrosini, V., & Bowman, C. (2001). Tacit knowledge: Some suggestions for operationalization. *Journal of Management Studies, 38*(6): 811–829. https://doi.org/10.1111/1467-6486.00260

Andriessen, D., & Bratianu, C. (2008). *Knowledge as energy: A metaphorical analysis.* Paper Presented at ECKM 2008, Southampton Solent University, Southampton.

Biggam, J. (2001). Defining knowledge: An epistemological foundation for knowledge management. *Proceedings of the 34th Annual Hawaii International Conference on System Science*s, 7. https://doi.org/10.1109/HICSS.2001.927102

Davenport, T. & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business School Press.

Esler, K. J., Prozesky, H., Sharma, G. P., & McGeoch, M. (2010). How wide is the "knowing-doing" gap in invasion biology? *Biological Invasions*, *12*(12), 4065–4075. https://doi.org/10.1007/s10530-010-9812-x

Hansen, M. T., Nohria, N., & Tierney, T. (1999). What's your strategy for managing knowledge? *Harvard Business Review.*

Janse, B. (2019). Nadler-Tushman Congruence Model. Toolshero. https://www.toolshero.com/management/nadler-tushman-congruence-model/

Job Qualification Record for Defensive Cyber Operations Planner Basic Level. (2020, February). *Cyber Mission Force.*

Job Qualification Record for Defensive Cyber Operations Team Lead/ Deputy Team Lead Basic Level. (2020, February). *Cyber Mission Force*.

Joint Chiefs of Staff (JCS). (2018). *Cyberspace Operations* (Joint Publication 3-12). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Mercer Delta. 1998. *The Congruence Model: A roadmap for understanding organizational performance.* Mercer Delta Consulting LLC.

Nissen, M. (2013). *Harnessing dynamic knowledge principles in the technology-driven world*. IGI Global.

Nissen, M. (2014). *Harnessing dynamic knowledge principles in the technology-driven world*. IGI Global.

Pfeffer, J., & Sutton, R. I. (1999). Knowing "what" to do is not enough: Turning knowledge into action. *California Management Review*, *42*(1), 83–108. https://doi.org/10.1177/000812569904200101

Simms, J. R., & Johnson, P. J. (2012). Knowledge: A measurable universal phenomenon of life. *Systems Research and Behavioral Science*, 29(4), 448–456. https://doi.org/10.1002/sres.2114

Smith, E. A. (2001). The role of tacit and explicit knowledge in the workplace. *Journal of Knowledge Management*, *5*(4), 311–321. https://doi.org/10.1108/13673270110411733

Stoney, T., Hoffman, R., Merritt, D. & Smith, S. (2019). Modelling the cognitive work of cyber protection teams. *The Cyber Defense Review*, *4*(1), 125–136.

U.S. Army Logistics. (2016). HIP-pocket guide. https://api.army.mil/e2/c/downloads/495919.pdf

U.S. Army Cyber Command (ARCYBER). (2020, February 10). *DOD fact sheet: Cyber mission force*. https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet(-cyber-mission-force/.

U.S. Department of Defense (DOD). (2016). All Cyber Mission Force Teams achieve initial operating capability. https://www.defense.gov/Explore/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/#:~:text=All%20133%20of%20U.S.%20Cyber,21%2C%20Cybercom%20officials%20announced%20today.&text=Reaching%20the%20IOC%20milestone%20is,DOD's%20Cyber%20Strategy%2C%20officials%20said.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California