Multiple Hypothesis Tracking of a Cyber Threat

Brett Tucker PMP, CSSBB, CISSP

Natasha Shevchenko

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0466

Problem to be Solved

How do you track a cyberthreat in an already compromised network?

By a Unique Partnership…

Carnegie Mellon University

Topic:AFX20D-TCSO1

Proposal #: **FX20D-TCSO1-0073**

This Research Seeks to:

Predict the next move by a cyberthreat

Hypothesizes a cyberthreat's ultimate intent

Estimate the risk to the network.

Proposed Use Cases for Application

Important addition to your real-time operational command monitoring

Provides a simulation to assess a network's vulnerabilities

Uses as a "red-versus-blue" training tool

Increases CMMC compliance

Ultimately, This Project Seeks to Reduce Risk Exposure Through Threat Identification and Assessment.

How is This Solution Different?

Utilize proven tracking technology from missile defense to predict a threat's future moves – **THREAT ASSESSMENT**

Uses probabilistic methods to augment network data collection and processing to assess a potential threat – **THREAT IDENTIFICATION**

Provides a means to estimate threat behavior – **THREAT ASSESSMENT**

Why Do You Need It?

Current monitoring and training technology lacks the **ability to predict** where threats might go next.

Matching threat behavior to prior tactics databases is inadequate.

There is an inadequate number of skilled operators to monitor network activity.

- There is a need for dynamic training of new talent.
- Our aging expert workforce needs to be augmented by automation.

Long-Term Benefits

This Research Seeks to Provide

Significant **increase in the defensive capability** against cyber attacks.

Reduction in risk exposure to a successful cyber attack.

Reduction in manpower required for monitoring network activity.

Establishing a Business Case

Return on Investment

Areas for consideration:

- Increase in the readiness of networks
- Reduction in manpower required for monitoring
- Advancement in probabilistic simulation and modeling techniques

How the Model and Simulation Works

1. Movement in the Network observed by Intrusion Detection System (IDS)

2. Sensor Data = Discrete States (e.g., IP/Port Addresses in IDMEF alert format)

3. Forecast threat track vector using Multiple Hypothesis Method (MHM)

4. Using data association, select and save the most likely threat vectors

Detailed Statistical Methods

Probabilistic Relational Model (PRM) Framework used to develop tracking algorithms

Threat movement modeled using a **Dynamic Decision Network (DDN)** with Multi-Tactics & Trafficability

Bayesian Inference extended using **Second Order Uncertainty (SOU)** to increase precision of the forecast

Uses **Tactics DB from MITRE ATT&CK Framework** as a guide for potential threat maneuvers

Perceived value of target assets used as a **weighting factor to hypothetical path selection**

Discrimination and Validation

This approach is different from today's technology:

- Adds the ability to predict the likely next move in the attack vector using Multi Hypothesis Method (MHM) within a Bayesian framework.

Validation of the feasibility of the approach:

- **Phase I:** Use a simplified simulation of a cyber attack with a single intruder with a limited number of maneuver tactics.
- **Phase II:** Validation and certification determined by real-time penetration testing.

Specifics Regarding Participation

Development team for the effort includes:

- **GCAS**: Over 40-years DoD Provider in AI Technology
- **Carnegie Mellon University SEI**: #1 University in Cyber and AI
- **Lockheed-Martin**: Leader in AI Defense

AFWERX will provide funding up to $750K with a MOU (Memo of Understanding).

Any Funding required **beyond** the $750K AFWERX Ceiling is provided by your Organization.

- Future funding needed only after proof-of-concept is validated.
- Multiple government agencies can collaborate to share future funding needs.

How to Advance this Research

Agree to a Memo of Understanding (MOU)

- Assign an Air Force employee as the Technical Point of Contact (TPOC) from our organization
- TPOC will actively participate in the Phase II follow-on effort

Commitment of **funds** for Phase II is **optional**.

Points of Contact

C. Thomas (Tom) Savell
CEO, GCAS Incorporated
ctsavell@gcas.net

1531 Grand Avenue, San Marcos CA 92078
(760) 591-4227
www.gcas.net (Government);
www.gcas.com (Commercial)

Brett Tucker, PMP, CSSBB, CISSP
Technical Manager, Cyber Risk Management
Carnegie Mellon University
Software Engineering Institute||CERT
batucker@sei.cmu.edu
(412) 268-6682
www.sei.cmu.edu

Backup Slides

Overall Summary

This Proposal addresses the **tracking and forecasting a cyber threat's future maneuvers in a compromised network**

Our approach includes:

- Movement in the network observed by Intrusion Detection System (IDS)
- Sensor Data = Discrete States (e.g., IP or Port Addressed per IDMEF [1] Alert Format)
- Forecast Threat Track Vector using Multiple Hypothesis Method (MHM) [2-6]
  - Use Probabilistic Relational Model (PRM) [7] Framework to Develop Tracking Algorithms.
  - Model Threat Movement using a Dynamic Decision Network (DDN) [8] with Multi-Tactics & Trafficability [9]
  - Extend Bayesian Inference with Second Order Uncertainty (SOU) [8, 10] => Increased Precision
  - Select Multiple Hypothesis of Movement Tactics from MITRE ATT&CK Framework [11-12]
  - Apply Weight to Hypothesis Path based on Value of Target Assets [13]
  - Using Data Association [14, 15] Select and Save the Top-3 Likely Threat Vectors for Further Tracking

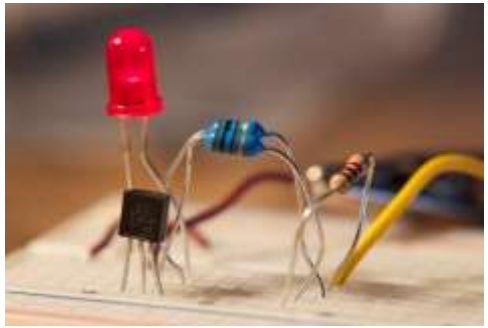
Summary (continued)

How is this different from Today's Technology?

- Identifies and assesses threats to predict the likely next move in the attack vector using MHM

Phase-I validation of the method using a simplified simulation of a cyber attack

- Single intruder with a limited number of maneuver tactics



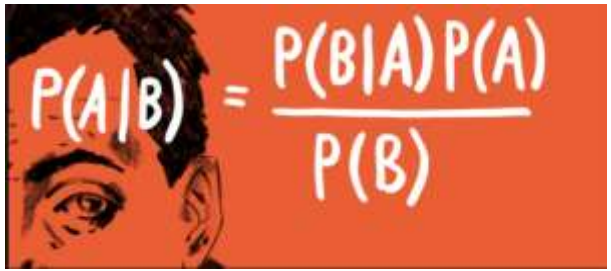
Recursive Dynamic Bayesian Network

Dynamic Decision Network (DDN) to Recursively update Threat's Forecasted Future Movement

- Discrete Data for States (Tactics/Nodes)
- Interacting Multiple Model (IMM) Filter [5]
- Trafficability Weighting of Network Paths [9]
- Capture Uncertainty in Observations and the Uncertainty in Threat's Maneuvering Process

Use Probabilistic Relational Models (PRMs)

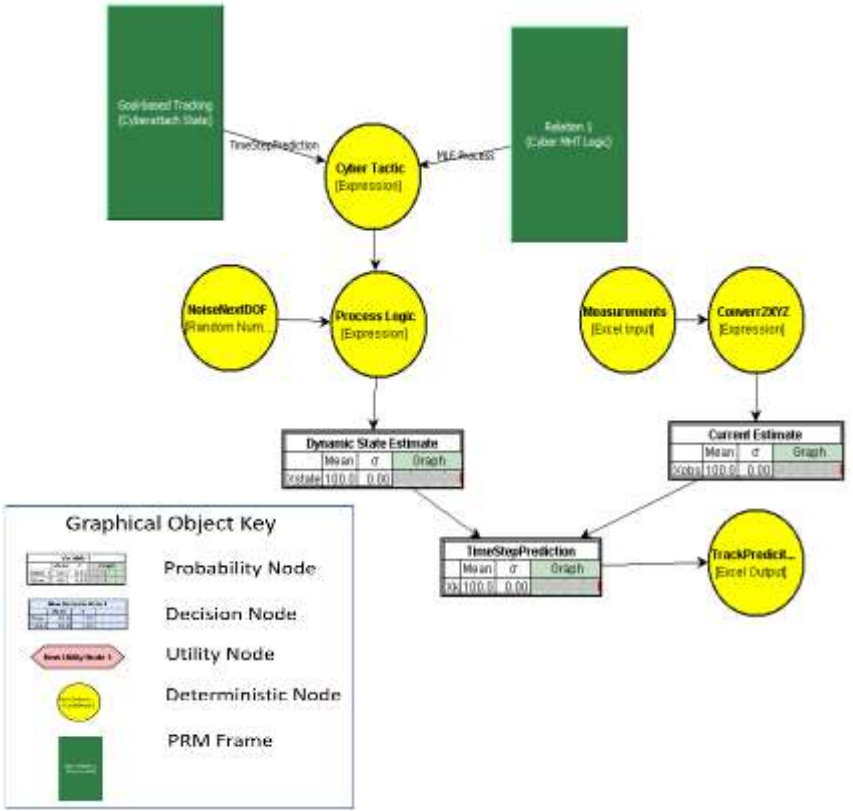
- Recursive Time Progression
- Modular Object-Oriented Design Architecture
- Additional Forms of Uncertainty [7]



Recursive Dynamic Bayesian Network (continued)

Multiple Possible Attack Processes

- Multiple Sensor Correlations & Tactics
- Goal-based Tracking [13] Approach:
  - Weight Defensive Maneuver based on Asset Value
- Uncertainty Propagation in All Steps



Interacting Multiple Model (IMM) Filter

Designed for Tracking Objects that are Highly Maneuverable.

Used to:

- Predict the future location of an object
- Reduce noise in the detected location, and/or
- Help associate multiple object detections with their tracks

Multiple motion ("Process") models in the Bayesian framework.

- **Radar Tracking**: Various possible kinematic state motions that could be performed by the tracked target (e.g., Constant Velocity, Constant-G Turn, etc.)
- **Cyber Tracking**: Various possible transitions between sensors/locations that could occur as represented by finite changes in state (Transition Matrix)

Interacting Multiple Model (IMM) Filter (continued)

Resolves the target motion uncertainty by using multiple models at each time step for a maneuvering target.

The IMM algorithm processes all the models simultaneously and switches between models according to their updated Probabilistic Weights (Scores).

Cyber Multiple Hypothesis Method (MHM)

Use DDN with Utility and Decision Nodes

Use MHM for Maintaining Likely Future Moves

Large Number of Possible Correlations

- Unknown a priori
- New Attack Strategies are Possible
- Independent of Domain Knowledge
- Use Evidence from:
  - Network Sensors
  - Non-Security Sources (e.g., NMS)

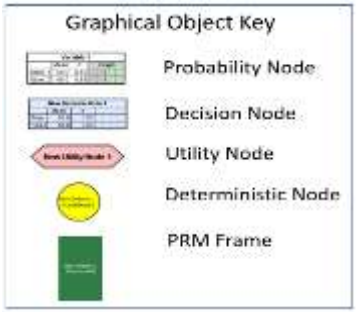
Value Weighting of Asset Targets

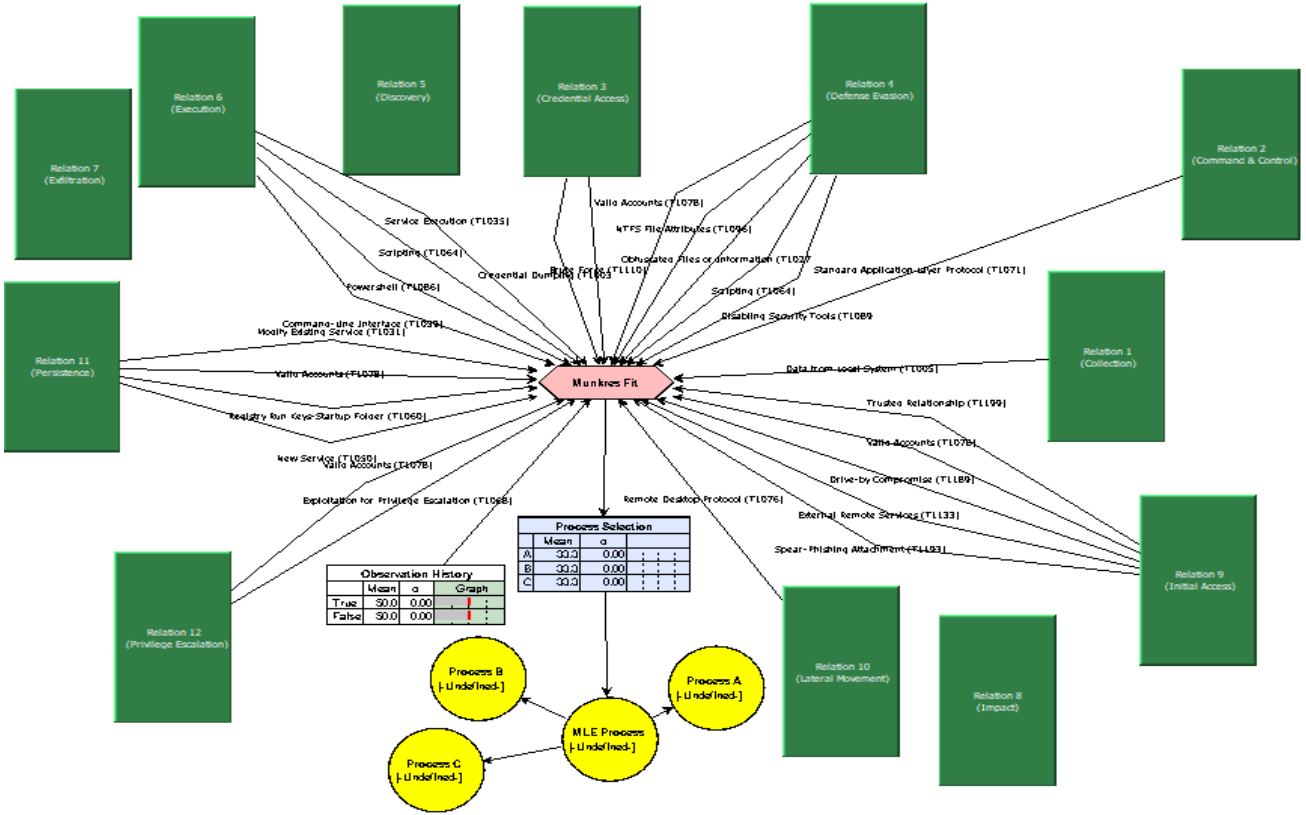
Example Attack Tactics = Discrete Process

- Reconnaissance
- Commencement
- Entry
- Foothold
- Lateral movement

- Acquire control
- Acquire target
- Implement/execute
- Conceal & Maintain
- Withdraw

Cyber Multiple Hypothesis Method (continued)





Cyber MHM Tracking Analogies

MHM Tracking of a Cyberthreat Analogous to Tracking a Target in Missile Defense

- Based on the Immediate Circumstances

Function	Kinematic Tracker	Cyber Tracker
Observations	Sensors (radar, EO, etc.) produce physical measurements of range, angle, attributes, etc. with measurement errors, SNR, etc.	Cyber sensor (e.g. intrusion detection system) detects anomalous events with confidences based on degree of deviation from the norm.
Data Type	Generally continuous data that can have any numerical value	Limited to a finite set of discrete states (albeit possibly a large number of finite states).
Track Formation	Formed from observations that have consistent kinematics and attributes. Scoring based on kinematics and attributes	Linked sequences of events that are part of a potential hostile attack. Scoring based on consistency of events leading to a goal state and the match to assumed templates.
Prediction and Filtering	Simple laws of physics Multiple assumed maneuver models	Comparison with templates and perceived system vulnerability Multiple template models
Hypothesis Formation	Sets of compatible tracks that do not share observations	Sets of tracks (linked sequences of events) that lead to compatible goal states.
Resource Management	Based on tracking error and track priority	Prioritization based on system vulnerability to perceived attack.

Validate with Simplified Cyber Attack Simulation

Verify MHM Approach with Simple Cyber Attack Simulation (e.g., MATLAB)

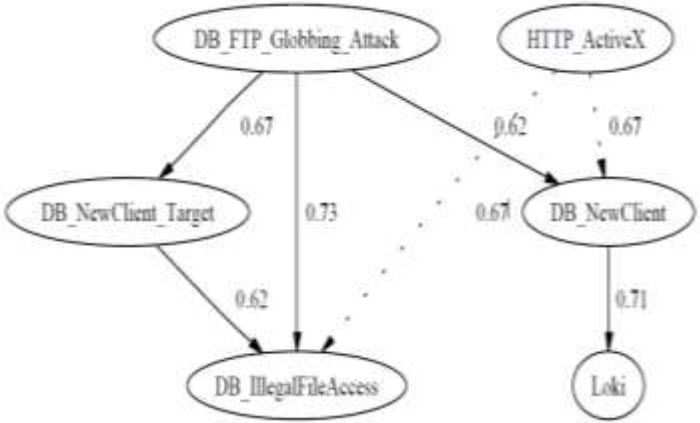
DARPA Grand Challenge Problem (GCP)

Use Output from Alert Correlation System for Sensor Observations

Assign Trafficability [9] Weights to Network Paths

Correlate Attack Steps to Security Steps

- Direct Correlation (Port Scan => Buffer O/F)
- Use Partial Correlation Evidence
- Use Temporal Statistical Patterns/Anomaly Detection
- Use Limited Reduced List of Tactical Maneuvers



Validate with Simplified Cyber Attack Simulation (continued)

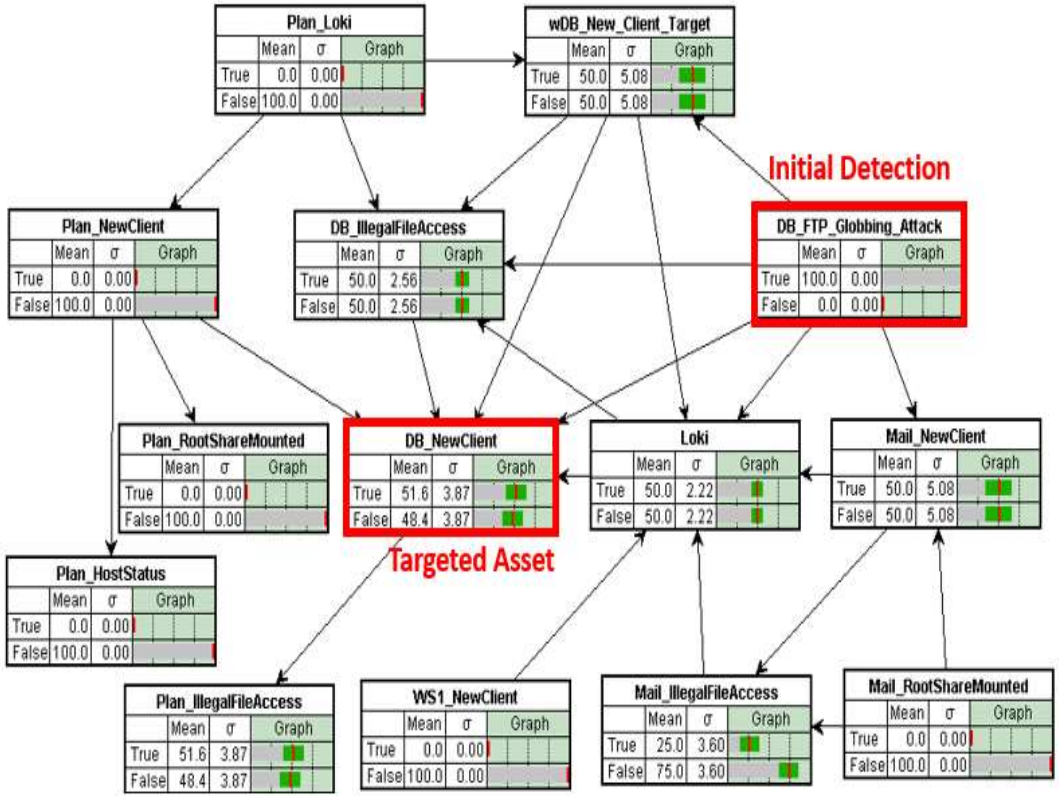
Assign a Weight to the Asset Value [13]

Apply Data Association [14,15] to MHM Threads

Determine Relative Maneuver Likelihoods

Conduct Monte-Carlo Simulations

- Obtain Statistics of Metric Measures
  - Number of False Negatives
  - Number of False Positives



Technical Merit

Significant industry need for our two future Phase-III products

1. Efficient Algorithms using MHM for Predicting Future Movement of Cyberthreat
2. Cyber Simulation & Modeling (S&M) Tool for CMMC Compliance

MHM is a Widely Used and Proven Methodology in Kinematic Target Tracking [2-6]

- Low Technical Risk
- Previously Proposed for Cyberattacks [16-18] But Never Adopted/Developed due to:
  - Lack of a Demonstration of Its Merits
  - No “Real-time” (or even fast) Monitoring, Detection and Tracking of a Threat Exists Today
  - Despite IDS Technology is Rapidly Advancing

Future Phase III Need = Create a Cyber Threat Simulator for CMMC Compliance [19].

- At least 15 CMMC Requirements benefiting from an S&M Tool

The Team: GCAS, CMU and LMCO

GCAS

Small Business Specializing in **Predictive Data Analytics:**

- 39-years as a DoD Contractor
- Expertise in Predictive Data Analytics
- Numerous DoD Contracts in:
  - Target Tracking, Predictive Data Analytics, and Simulation & Modeling
- Numerous Prior Successful Product Commercialization with Army, Navy, MDA and Industry including:
  - SOU (Second Order Uncertainty) [8, 10, 20] used by MDA, Navy & DARPA for Ballistic Target Tracking
  - ACES S&M Tool [21] to predict the Deterioration of Wheeled Vehicles over Time (Army, Oshkosh, GM)
  - ESCAT (*Expert Structures and Coating Analysis Tool*) [22] for Scheduling Ship T&V Refurbishment (Navy)
  - GCAS Accounting Suite [23] sold to DoD Contractors for Job Costing and Project Management
  - VC100 PC-based Vibration Control System purchased by Navy and Industry

The Team: GCAS, CMU and LMCO (continued)

Carnegie Mellon University

- Leader in the Development of Advanced AI Methods
- #1-ranked School of Computer Science
- CyLab consists of 30 core and 60 affiliated faculty with over 400 Publications
- Cyber Winners: DefCon (5-times), DARPA Cyber Grand Challenge, & DefCon Crack-Me-If-You-Can
- FFRDC “Software Engineering Institute (CMU-SEI) with CERT Division

Lockheed Martin Corporation

- Top Defense Contractor (110,000 employees) including 700+ Engineers in Cyber Innovations Alone
- Large Cyber Defense Infrastructure = CMMC Level-5 Appraised
- Developer of Cyber Attack Network Simulator (CANS) [24]

Ability to Perform Research and Commercialization

Phase I Project Scope and Timeline:

- Phase I is a Proof of the MHM Technique for Predicting a Threat's Next Maneuver
  - GCAS has developed a Predictive Analytics Modeling Framework with the SOU Software [8, 10, 20] needed for the Creation of the Cyberthreat Tracking MHM Algorithms
  - Extending the Existing SOU Framework can be Accomplished in the 6-month Phase-I Timeframe
  - Due to Time and Funding Limitations, Only a Proof-of-Concept Demonstration is Feasible in Phase-I
    - A Full Simulation and Modeling System is Proposed for Phase-II

Ability to Perform Research and Commercialization (continued)

Phase II Development and Phase III Commercialization:

- The Successful Outcome of Phase II is a Commercially Viable Wargaming S&M System Utilizing MHM
  - Our Team consists of the:
    - Leading Predictive Analytics Small Business,
    - #1 University in AI and Cybersecurity, and
    - #1 DoD Contractor.
  - Brings Experience and Reputation of Producing Quality Products
    - Understanding of the Technology
    - Understanding of the Marketplace, and
    - Experience in Commercializing Technical Solutions
  - Work with and know Personally the End-Users for our Proposed Phase III Products.
    - Both Inside and Outside of the Government

Commercialization Potential

GCAS Track Record in Commercialization

- SBIR CAI = 70;
- Multiple DoD Users of GCAS Developed Products: ACES, ECAT, VC100
- Multiple Commercial Products: GCAS Accounting Suite, ACES, VC100, MAC, etc

Two Phase III Products:

1) MHM Technology in Cyberattack Modeling
2) Cyber S&M System

Commercialization Potential (continued)

Market for MHM Technology in **Cyberattack Modeling**

- Technology that can Forecast the Threat's next likely Movement within the Network:
- Sell or License Technology to Existing Cybersecurity Companies
- Sell or License to integrate into Network Detection and Response (NDR) Vendors

Market for Simulation and **Modeling System for Wargaming Cyberthreat on Assets**

- Standalone Simulation Tool based on AFSIM, CANS, PASTA, DoDAF, SysML, Cameo
  - GUI for Users to Configure Their Network Architecture, including Ports, Sensors, etc.
  - Renewable Database of Known Threat Maneuvers per MITRE ATT&CK Framework [11-12]
  - Database of Known Threat Attack Case Studies
  - Developed Decision Network Algorithms for Predicting Various Possible Threat Movements.
- Direct Sales to Government and Industry
  - Huge Potential Market by Addressing CMMC Compliance Requirements

Commercialization Potential (continued)

15 CMMC Compliance Requirements Benefiting from Simulations

CMMC Best Practices Naming Convention: [DOMAIN].[LEVEL].[PRACTICE NUMBER]

- Domain:
  - Incident Response (IR)
  - Risk Management (RM)
  - Security Assessment (CA)
  - Situation Awareness (SA)

- Level
  1. Basic Cybersecurity
  2. Accepted Best Practices
  3. All NIST SP 800-171 rev-1
  4. Advanced & Sophisticated
  5. Highly Advanced

CMMC	Description
IR.2.097	Perform root cause analysis on incidents to determine underlying causes
IR.3.099	Test the organizational incident response capability
IR.4.100	Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution
IR.5.102	Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns
RM.2.142	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified
RM.3.144	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria
RM.4.150	Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries
RM.5.155	Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence
CA.2.158	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application
CA.3.161	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls
CA.4.164	Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts
CA.4.227	Periodically perform red teaming against organizational assets in order to validate defensive capabilities
SA.4.171	Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls
SA.4.173	Design network and system security capabilities to leverage, integrate, and share indicators of compromise

Significance of the Problem and Opportunity

Addresses the Existing Need to **Predict the Movement of a Cyberthreat** in a Compromised Network

Extends the Current State-of-the-Art in **Cyberthreat Modeling and Wargaming**

Provides the **Foundation for a Future Commercial Cyberwarfare Simulator** needed in Industry to meet the CMMC Compliance Requirements

Phase I Objectives

Achieve a High TRL Proof-of-Concept within a Compressed 6-month Timeline

Develop Methods to Predict Cyberthreat Movement in a Compromised Network

- Use Existing Bayesian Methods (BN, DN, PRM, SOU)
- Use Multi Hypothesis Method (MHM)
- Leverage Existing GCAS Software Tool to Achieve End Result with High TRL =4 in Phase II

Phase I Objectives (continued)

Measure of Success in Achieving Performance from Phase I Algorithm Development

- Validate the Algorithms using a Simple Prototype Demonstration
  - Develop Simulator in MATLAB
  - Track a Single Cyberthreat Through a Simple Network Structure (See Slide #7)
  - Use DARPA Grand Challenge Problem (GCP) Threat Scenario
- Conduct 1000's of Monte-Carlo Runs with Different Possible Outcomes
- Document the Accuracy and Precision of the Predicted Threat Movement with Measures:
  - Number of False Negatives
  - Number of False Positives

Phase I Algorithm Basis for Phase-II Product Development

Phase I Commercialization Task Identify and Start Dialog with Phase III Customers for

- Licensing Cyberthreat MHM Technology
- Purchase of Wargaming Simulation and Modeling System for CMMC Compliance

Related Work - Dual-Use

PI, Dr. Tom Savell, Designed GCAS' SOU BN/DN/PRM Modeling System & ACES S&M System

- SOU was Developed and Used on the Following DARPA, MDA and Navy Efforts:
  - Ollie Allen (retired); Navy PMA-290; 301-757-5697; c7f1999@gmail.com; (2019) ,
  - Robert Rumbaugh; Navy IWS-1, robert.rumbaugh@navy.mil; 202-781-4932; (2018) ,
  - Dr. Karla Spriestersbach; MDA BC/BCDV; 256-450-3289; Karla.Spriestersbach@mda.mil (2018)
  - Dr. John Crigler (retired), Navy NSWC Dahlgren Division (for DARPA); 540-653-7601; criglerjr@nswc.navy.mil, (2007)
- ACES S&M System was Developed and Used under the Following Army and Navy Contracts and used by the Army, Oshkosh and General Motors:
  - Scott Porter, Army TARDEC 586-282-4373; scott.w.porter.civ@mail.mil (2020 Phase III work-in-process)
  - Craig Matzdorf, NAVAIR, 301-342-9372, craig.matzdorf@navy.mil (2013)
  - Alex Thiel, Oshkosh Defense, alexthiel@oshkoshcorp.com, (920) 235-9151 x25844 (currently in-house)
  - Larry Thompson, General Motors, larry.s.thompson@gm.com, 248-520-0810 (currently in-house)
- Relevance to the Proposed Cyberattack Modeling Effort
  - The SOU Modeling System will be Directly used on the Project to Develop the MHM Algorithms and Architecture
  - The Experience and Tools used to Develop the Parallel Processing ACES S&M System will benefit the Phase II Simulator Development

Related Work - Dual-Use (continued)

CMU has Numerous Contracts and Efforts in Cybersecurity including CERT and SEI

LMCO has Extensive Experience Running AFRL's AFSIM as a Standalone or Part of a Simulation Federation

LMCO Developed the Cyber Attack Network Simulator (CANS)

Both CMU and LMCO have Deep Insight into the Current Market to Advise GCAS

Relationship with Future Work

Our Phase I Effort will Lay Foundation for a Phase II Cyber Wargaming S&M System

- Use IDS Backbone (AFSim, CANS, PASTA, DoDAF, SysML, Cameo)
  - Extend with New MHM Tracking Technology
- Commercial Deployment
  - Tool for CMMC Compliance (Levels 2-5)
  - Use Database of Existing Documented Threat Maneuver Strategies for Hypotheses:
    - KDD Cup 99 Data Set,
    - Maze Ransomware Incursion

Relationship with Future Work (continued)

Successful Phase II Results in Highly Lucrative Phase III Commercial Product

GCAS Prime and CMU & LMCO Subs all have Classified Facilities As Required

Air Force Research Lab is a Key Acquisition Customer

- Integrate MHM Technology into the Existing AFSim [25] Architecture

Other Key DoD Customers include

- US Cyber Command, and
- Joint Artificial Intelligence Center

Numerous Industry and University Initiatives

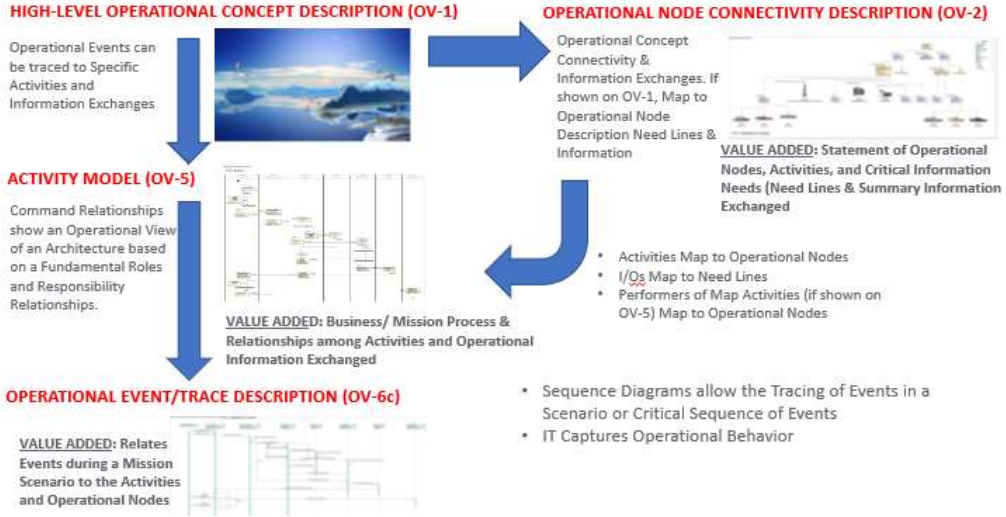
Develop Cyber Wargaming S&M System

Integrate our MHM Logic into An Existing Threat Modeling Systems [24-28]

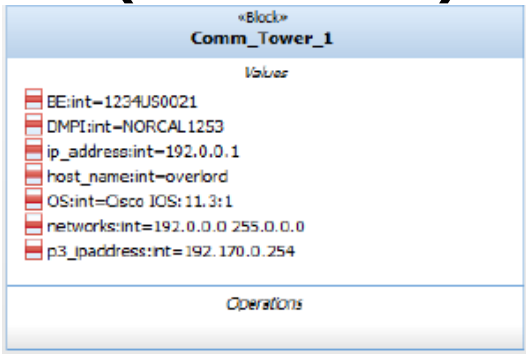
- AFSIM [25] Guidance + LMCO CANS [24] Insight
- PASTA for high level inputs and Framework Procedure => Data Flow Diagram
- DoDAF Architecture Framework for Enterprise Level View
- SysML Diagrams (Block Definition=BDD & Internal Block=IBD) to populate System Level
- Cameo Modeling Environment (Enterprise Architecture, System Modeler)

Develop Simulation of Cyber Attack for Testing the Approach

Develop Cyber Wargaming S&M System (continued)



DoDAF Architecture



CANS GUI Presentation

Commercialization Strategy

A Successful Phase II Development will Result in 2 Commercial Products:

1. MHM for Cyberattack Modeling Technology and Algorithms, and
2. Simulation and Modeling Tool for Wargaming Cyberthreats on Assets to Addresses CMMC Compliance

Customers and Market Size:

- Within the Air Force the Primary Customer for the Technology is the Air Force Research Lab
- Other DoD Agencies of Interest include US Cyber Command, and Joint Artificial Intelligence Center
- Industry Customers for the Technology is estimated to be in the 100's are:
  - Cybersecurity Companies
  - Network Detection & Response Vendors
- Industry & Government Market for S&M Tool for Wargaming Simulations is estimated to be in the 10,000's
  - Includes All US Government Contractors needing to Achieve CMMC Compliance + Potential World-Wide Market

Commercialization Strategy (Continued)

Funding Requirements for Commercialization

- Pricing = $10K to $100K /unit depends on demand
- Primary Expense is Sales & Marketing
- Cash Infusion of $2.5M Required from Investors
  - 6:1 initial ROI from Initial Introduction
  - Reinvest for Future Continued Growth

* = Phase II Funds	Phase II		Phase III				
	Year 1	Year 2	Year 1	Year 2	Year 3	Year 4	Year 5
Expenses	$476K	$476K	5M	5M	5M	5M	5M
Sales/Service Revenue	--	--	4M	4M	8M	10M	16M
External Investments	$500K*	$500K*	2.5M	0	0	0	0
Distribution to Investors	--	--	--			5M	10M
Profit/Loss	$24K	$24K	1.5M	-1M	3M	5M	11M

Commercialization Risks

- Only 5-7% of Technology Ventures Succeed
- Need to Acquire Outside Marketing Expertise

Formattable Competition from Cybersecurity Companies and Network Detection & Response Vendors

Risk Factor	Level	Justification
Produce Expected Output in a Business Environment	Low	Phase II Product development & testing
Transferring the Product to the Target Group	High	May Involve Profit Sharing/JV/Spinoff
Value creation	High	Creation of Market Awareness and Monetary Value
Customer Acceptance	Medium	CMU and LMCO Partners = Credibility
Capital market access	High	Finding investors and partners is critical
Intellectual property protection	Medium	SBIR Rights + Decision on IP Protection

Key Personnel

C. Thomas (Tom) Savell, GCAS Inc. (PI):

Tom is the founder and current CEO of GCAS with over 50 years experience in the DoD industry. He is designer of GCAS' suite of AI software products including the SOU Bayesian statistical modeling system used by MDA and the Navy, ACES simulation and modeling system used by the Army TARDEC/TACOM, Oshkosh Corporation and General Motors, ESCAT structure and coating deterioration prediction system used by Navy PEO-Carrier Planning Group, and the GCAS accounting software suite used by numerous DoD contractors. Prior to founding GCAS in 1981, he was the Technical Director for Structural Dynamics Research Corporation, Head of Advanced Products for Solar Turbines International, and Department head for General Electric AEG's Dynamic Analysis and Testing Group. He is the recipient of GE's Young Engineer of the Year award. He has a PhD is from the University of Cincinnati and a BS and MS from Ga Tech. He is a Guggenheim, Ford Foundation & NASA Fellow.

Brett Tucker, PMP, CSSBB, CISSP, CMU Cybersecurity Risk Expert:

Brett Tucker, PMP, CSSBB, is the Technical Manager of Cybersecurity Risk at Carnegie Mellon University's SEI. Tucker has 19 years of experience in the public and private sectors. Prior to joining the SEI, Tucker was the Global Risk Manager for Westinghouse where he managed the corporate enterprise risk portfolio and global insurance programs. Prior to Westinghouse, Tucker served as an Intelligence Officer at the CIA and is also a veteran of the US Navy Nuclear Propulsion Program. Tucker holds a degree in chemical engineering from the University of Notre Dame, a master's degree in engineering management from Old Dominion University and an MBA from Penn State University.

Key Personnel (continued)

Natasha Shevchenko, CMU Cyber Threat Modeling Expert:

Ms. Nataliya Shevchenko is Member of Technical Staff at Carnegie Mellon University (CMU) Software Engineering Institute (SEI) CERT division. She specializes in System Engineering, Model-Based System Engineering (MBSE) and Threat Modeling Methods. Nataliya has a breadth of experience across Software Development Life Cycle for 20+ years. Prior to joining SEI, she worked in teleconferencing, railroad and banking industries. Ms. Shevchenko holds MS degree in Software Engineering from Carnegie Mellon University, and BS and MS degrees in Mathematics from Donetsk State University in Ukraine.

Ambrose Kam, LMCO Cyber Threat Modeling Expert:

Ambrose is Lockheed Martin Fellow with over 25 years experience in the Department of Defense (DoD) industry. He is one of the earliest pioneers at applying modeling, simulation and operations analysis techniques to threat modeling and cyber resiliency assessment. He regularly gives lectures at MIT, Georgia Tech and industry consortium like the Military Operations Research Society (MORS) and National Defense Industry Association (NDIA). Ambrose has been quoted in major publications including Forbes, The Economist, etc. His most recent efforts are in wargaming, machine learning/deep learning, Cyber Digital Twin and blockchain earned him patents and trade secret awards. In 2017, Ambrose won the prestigious Asian American Engineer of the Year (AAEOY) award for his technical leadership and community services. He holds several advanced degrees from MIT and Cornell University.

Registrations

GCAS

- DUNS Number: 118594928
- CAGE Code: 6W067
- SBA ID: 000172131
- DOD STTR ID: FX20D-TCSO1-0073

Carnegie Mellon University

- DUNS Number: 05-218-4116
- CAGE Code: 97668

Lockheed Martin Corporation- RMS (Moorestown, NJ)

- DUNS Number: n/a
- CAGE Code: 02769

Facilities and Equipment

GCAS:

- In Phase I GCAS will be Responsible for the Software Development of the MHM Algorithm and Design of the Proof-of-Concept Demonstration.
- GCAS has Multiple Computer Workstations used by its Staff including GPU-based Parallel Processing Systems which may be required for the More Complex Modeling Effort in Phase II
- GCAS has Multiple Commercial and In-House Developed Modeling Tool's such as GCAS's SOU [8, 10] and Commercial MATLAB, Netica and Hugen DN Modeling Systems

Carnegie Mellon University:

- In Phase I, CMU will assist in the Design of the MHM Architecture by providing Insight into the Threat Attributes and Historical Vector Maneuvers and Tactics. To this end the Significant Database Resources found within CMU will be utilized
- In Phase II, CMU will tap into its Library of Existing Threat Modeling Software Tools to help in the Prototype Design and Development as well as its Database of Historical Threat Attack Processes needed for the MHM Software and the S&M System Development [19, 26, 27].

Facilities and Equipment (continued)

LMCO-RMS (Moorestown):

- In Phase I, LMCO will act as an Advisor to GCAS and CMU as to End-User Needs and Requirements.
- In Phase II they will participate in the S&M System Development contributing Their In-House Resources for Cyberthreat Modeling, including Knowledge of the Existing LMCO CANS System [24].
- LMCO-RMS Computer Resources include the MARS Supercomputer composed of:
  - 700+ engineers in Cyber Innovations alone
  - 8,000 Intel CPUs & 40 NVIDIA GPUs for Simulations and Visualize in GPE-Enabled Virtual Memory.
  - 240 NVIDIA GPUs for Accelerate Deep Neural Network (DNNs) Training; NVIDIA Strategic Partner
  - Data Lake – Read ML Datasets and Write Simulation Outputs to 1PB Super-Fast Storage

Acronyms

ACES: Accelerated Corrosion Expert System (GCAS commercial SW)
AFSIM: Air Force Research Laboratory's M&S Tool
ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge
BN: Bayesian Network
CA: Security Assessment CMMC Domain
CAI: Commercialization Achievement Index (SBIR Measure of Success)
CAMEO: Cyber System Modeling Tool (Commercial SW)
CANS: Cyber Attack Network Simulator (LMCO SW Product)
CERT: CMU's Certification Division
CMMC: Cybersecurity Maturity Model Certification
CMU: Carnegie Mellon University
CyLab: CMU's Security and Privacy Research Institute
DARPA: Defense Advanced Research Projects Agency
DBN: Dynamic Bayesian Network (BN that varies with Time)
DefCon: Defense Readiness Condition Cyber Hacker Convention
DN: Decision Network (BN + Decision and Utility Nodes)
DDN: Dynamic Decision Network (DN that varies with Time)
DoDAF: Department of Defense Architecture Framework
DoD: Department of Defense
ESCAT: Expert Structures & Coating Analysis Tool (GCAS commercial SW)
FFRDC: Federally Funded Research and Development Center
GCAS: SB Company Name ("Government Cost Accounting System" SW)
GCP: Grand Challenge Problem
GUI: Graphical User Interface
IDMEF: Intrusion Detection Message Exchange Format
IDS: Intrusion Detection System
IP: Internet Protocol
IR: Incident Response CMMC Domain
KDD Cup: Data Mining and Knowledge Discovery Competition LMCO: Lockheed Martin Corporation
MAC: Multiple Accelerator Controller (GCAS Commercial SW)
MATLAB: Mathematical Laboratory Simulation System
MAZE: Sophisticated Strain of Windows Ransomware
MDA: Missile Defense Agency
M&S: Modeling and Simulation
MHM: Multiple Hypothesis Method
NDR: Network Detection and Response
NIST SP 800-171: National Institute of Standards and Technology Special Publication
NMS: Network Management System (i.e., Non-Security Sources)
O/F: Overflow
PASTA: Process for Attack Simulation and Threat Analysis (Commercial SW)
PRM: Probabilistic Relational Model
RM: Risk Management CMMC Domain
RMS: LMCO Rotary and Mission Systems Division
SA: Situation Awareness CMMC Domain
S&M: Simulation and Modeling
SB: Small Business
SEI: CMU's Software Engineering Institute
SOU: Second Order Uncertainty (includes variance of uncertainty)
SW: Software
SySML: System of System Modelling Language based on UML 2. 0
TRL: Technology Readiness Level
VC100: Vibration Control System (GCAS commercial SW)