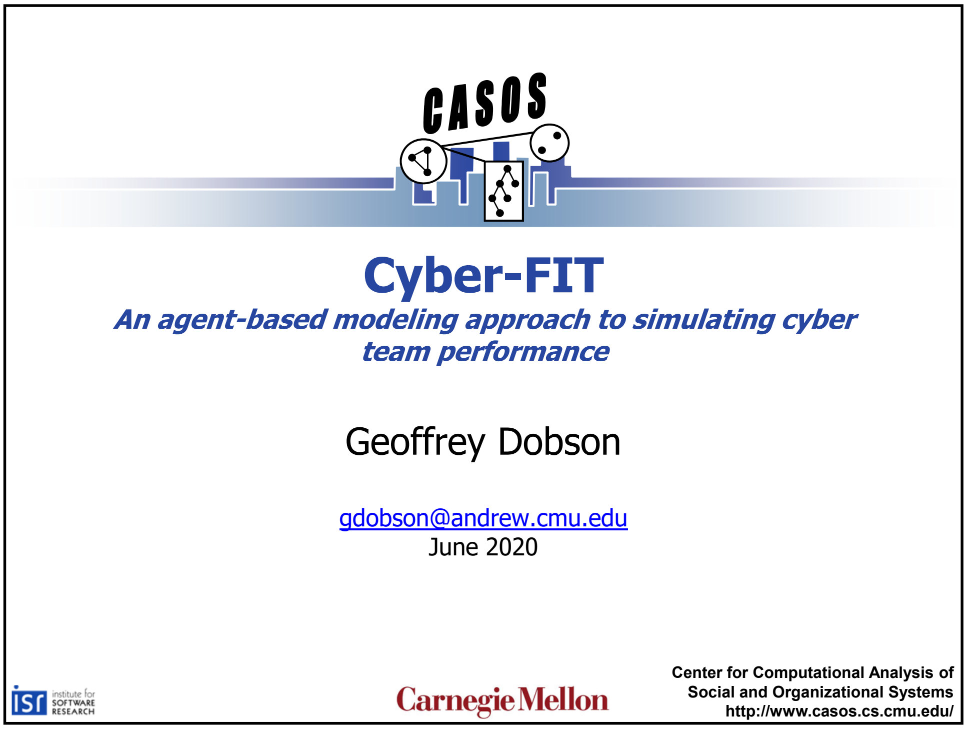


Cyber-FIT

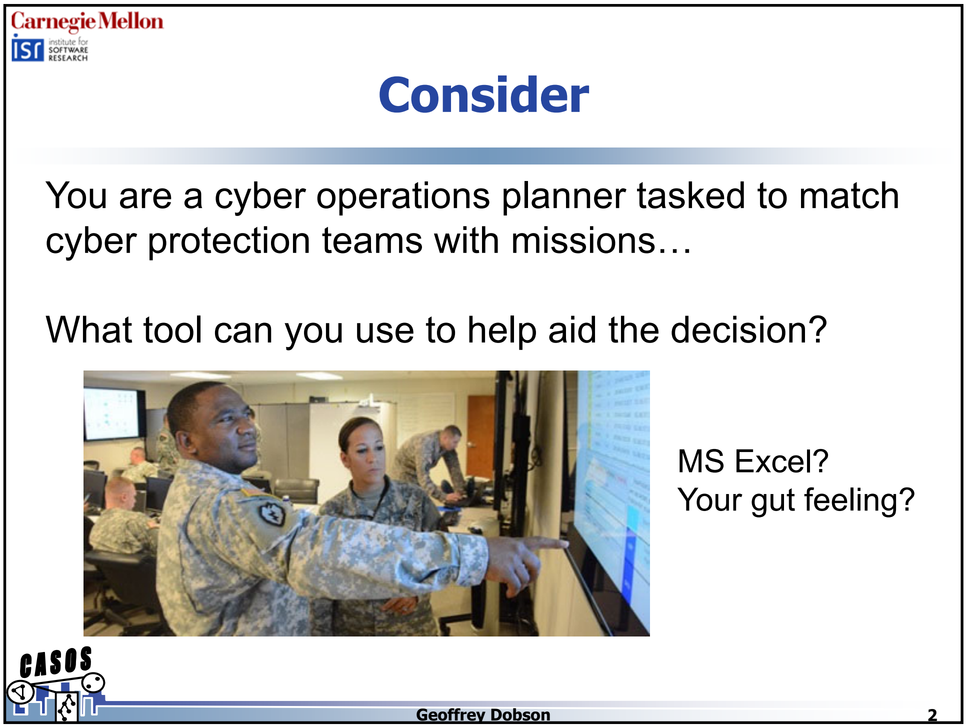
An agent-based modeling approach to simulating cyber team performance

Geoffrey Dobson

gdobson@andrew.cmu.edu

June 2020

Center for Computational Analysis of Social and Organizational Systems
http://www.casos.cs.cmu.edu/



Consider

You are a cyber operations planner tasked to match cyber protection teams with missions…

What tool can you use to help aid the decision?

MS Excel?
Your gut feeling?

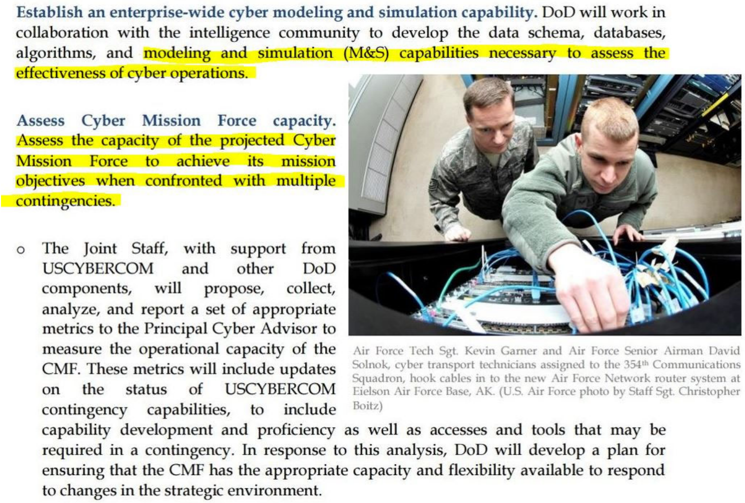
Consider

You are war-gaming a projected conflict with the DoD's most sophisticated simulation tool, OneSAF…

How do you simulate varying cyber team makeups in varying projected scenarios?

You can't

DoD Cyber Strategy



Establish an enterprise-wide cyber modeling and simulation capability. DoD will work in collaboration with the intelligence community to develop the data schema, databases, algorithms, and modeling and simulation (M&S) capabilities necessary to assess the effectiveness of cyber operations.

Assess Cyber Mission Force capacity. Assess the capacity of the projected Cyber Mission Force to achieve its mission objectives when confronted with multiple contingencies.

- The Joint Staff, with support from USCYBERCOM and other DoD components, will propose, collect, analyze, and report a set of appropriate metrics to the Principal Cyber Advisor to measure the operational capacity of the CMF. These metrics will include updates on the status of USCYBERCOM contingency capabilities, to include capability development and proficiency as well as accesses and tools that may be required in a contingency. In response to this analysis, DoD will develop a plan for ensuring that the CMF has the appropriate capacity and flexibility available to respond to changes in the strategic environment.

Air Force Tech Sgt. Kevin Garner and Air Force Senior Airman David Solnok, cyber transport technicians assigned to the 354th Communications Squadron, hook cables in to the new Air Force Network router system at Eielson Air Force Base, AK. (U.S. Air Force photo by Staff Sgt. Christopher Boitz)

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Defense Science Board Report

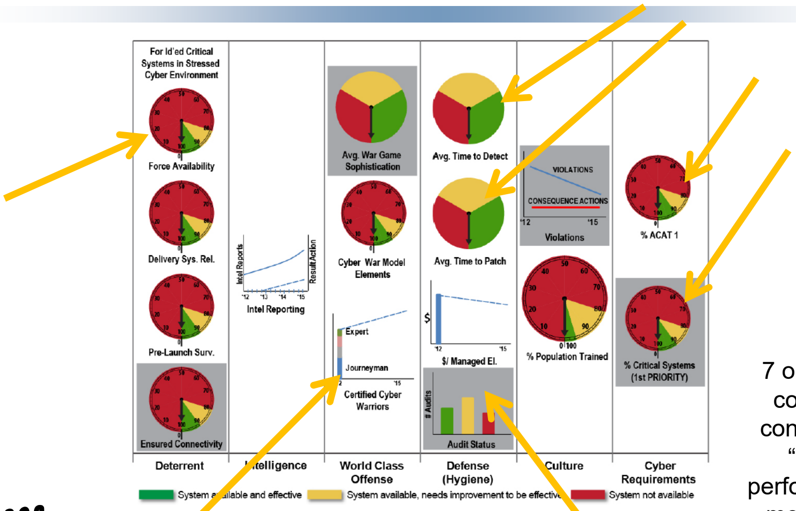


Figure 4.2 Notional Dashboard of System Performance Metrics

7 out of 16 could be considered "team performance" measures

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

DoD Cyber Training Budgeting

DoD

Army requests $429 million for new cyber training platform

By: Mark Pomerleau   February 21

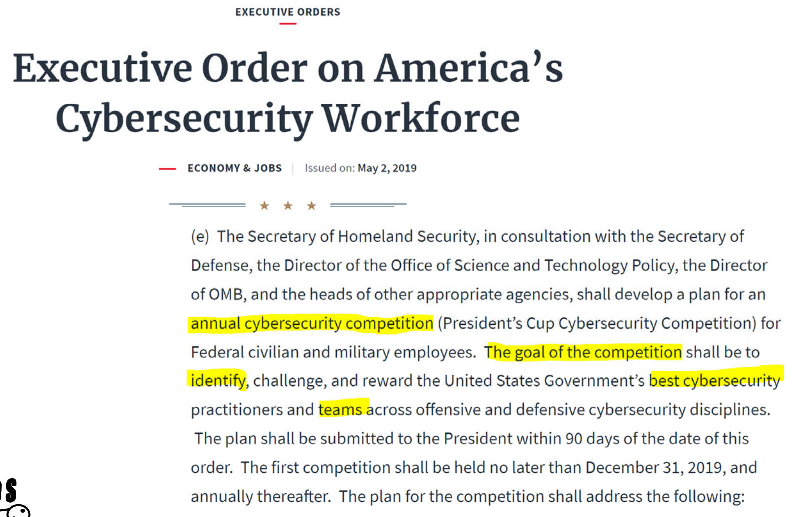
f G+ + 41

https://www.fifthdomain.com/dod/2018/02/21/army-requests-429-million-for-new-cyber-training-platform/

"several training exercises authorized for 2017 as part of the Combatant Commander Exercise Engagement and Training Transformation (CE2T2) program, funded at ***more than $150 million***"

https://prhome.defense.gov/Portals/52/Documents/RFM/Readiness/docs/Cyber%20Training%20in%20DoD%20FY2017%20budget.pdf

White House Executive Order



EXECUTIVE ORDERS

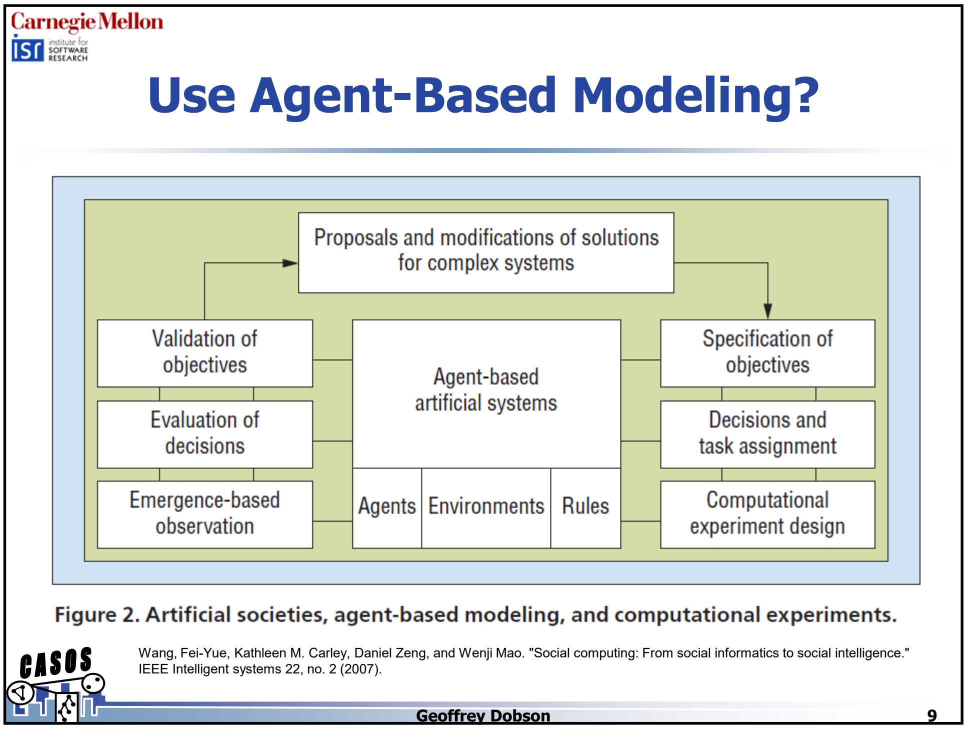
Executive Order on America's Cybersecurity Workforce

ECONOMY & JOBS | Issued on: May 2, 2019

★ ★ ★

(e) The Secretary of Homeland Security, in consultation with the Secretary of Defense, the Director of the Office of Science and Technology Policy, the Director of OMB, and the heads of other appropriate agencies, shall develop a plan for an annual cybersecurity competition (President's Cup Cybersecurity Competition) for Federal civilian and military employees. The goal of the competition shall be to identify, challenge, and reward the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines. The plan shall be submitted to the President within 90 days of the date of this order. The first competition shall be held no later than December 31, 2019, and annually thereafter. The plan for the competition shall address the following:

How to Measure Cyber Teams?



Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Use Agent-Based Modeling?

Proposals and modifications of solutions for complex systems

Validation of objectives

Evaluation of decisions

Emergence-based observation

Agent-based artificial systems

Agents | Environments | Rules

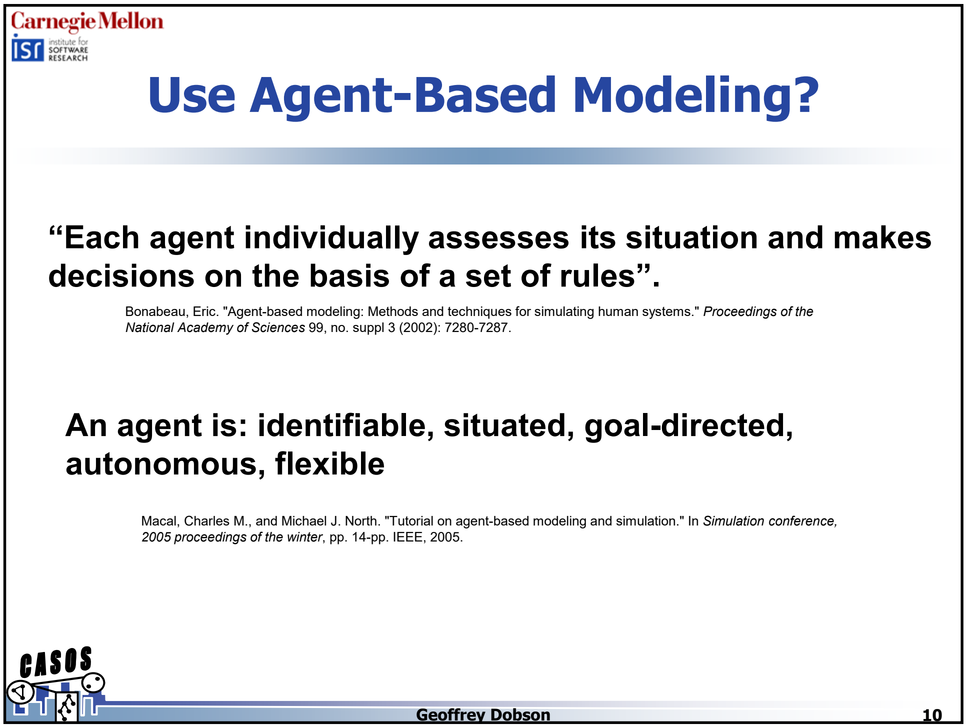
Specification of objectives

Decisions and task assignment

Computational experiment design

Figure 2. Artificial societies, agent-based modeling, and computational experiments.

Wang, Fei-Yue, Kathleen M. Carley, Daniel Zeng, and Wenji Mao. "Social computing: From social informatics to social intelligence." IEEE Intelligent systems 22, no. 2 (2007).



Carnegie Mellon
isr institute for SOFTWARE RESEARCH

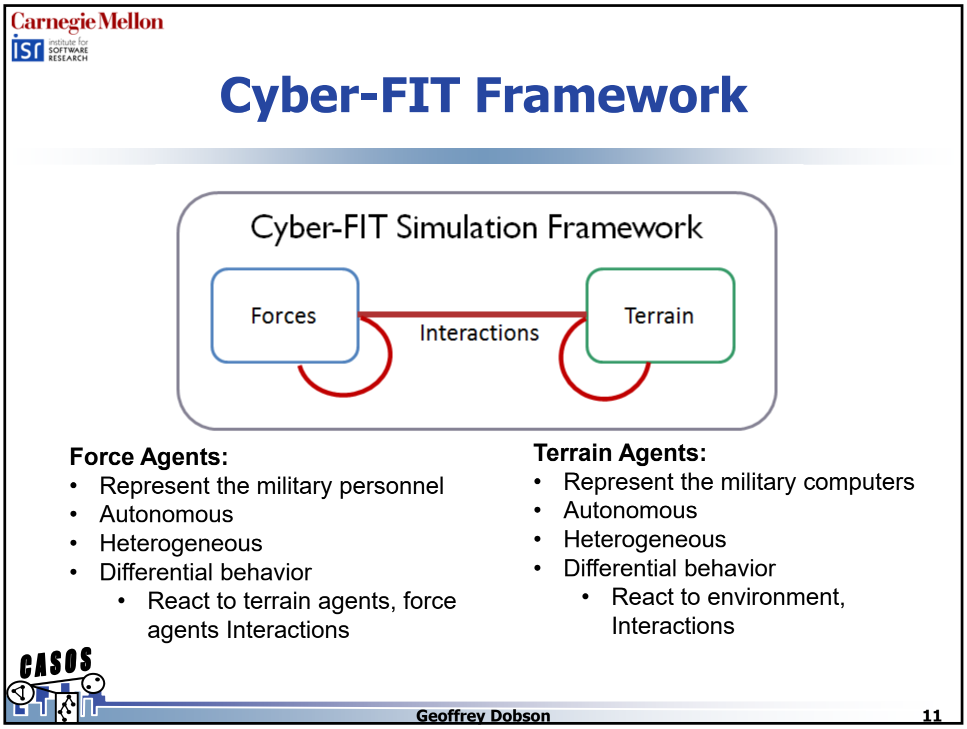
Use Agent-Based Modeling?

“Each agent individually assesses its situation and makes decisions on the basis of a set of rules”.

Bonabeau, Eric. "Agent-based modeling: Methods and techniques for simulating human systems." *Proceedings of the National Academy of Sciences* 99, no. suppl 3 (2002): 7280-7287.

An agent is: identifiable, situated, goal-directed, autonomous, flexible

Macal, Charles M., and Michael J. North. "Tutorial on agent-based modeling and simulation." In *Simulation conference, 2005 proceedings of the winter*, pp. 14-pp. IEEE, 2005.



Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Cyber-FIT Framework

Cyber-FIT Simulation Framework
Forces
Interactions
Terrain

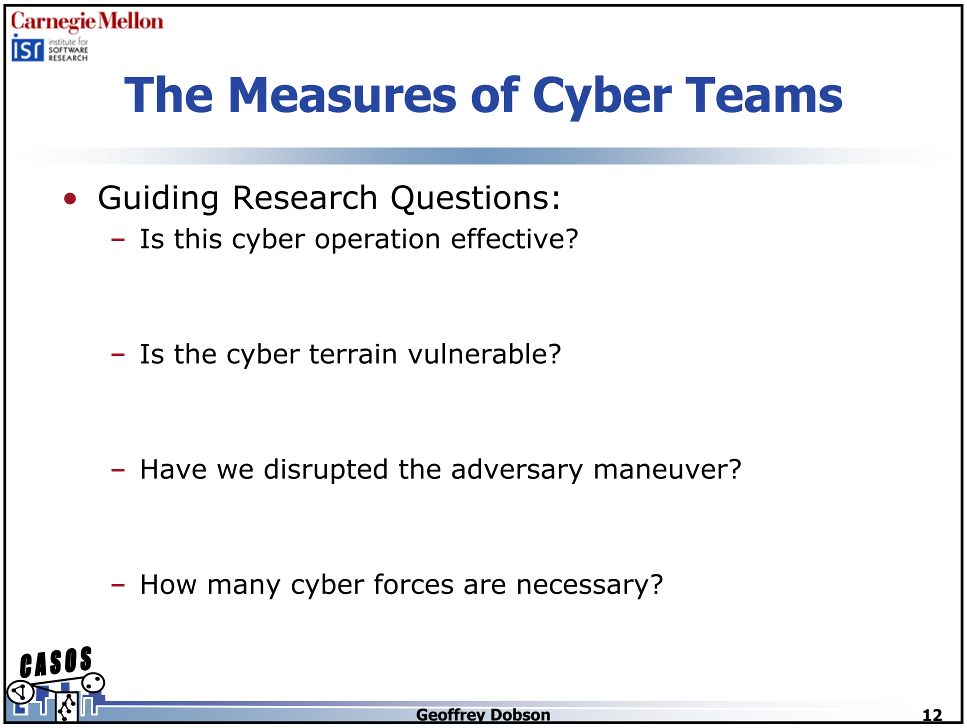
Force Agents:

- Represent the military personnel
- Autonomous
- Heterogeneous
- Differential behavior
  - React to terrain agents, force agents Interactions

Terrain Agents:

- Represent the military computers
- Autonomous
- Heterogeneous
- Differential behavior
  - React to environment, Interactions

CASOS

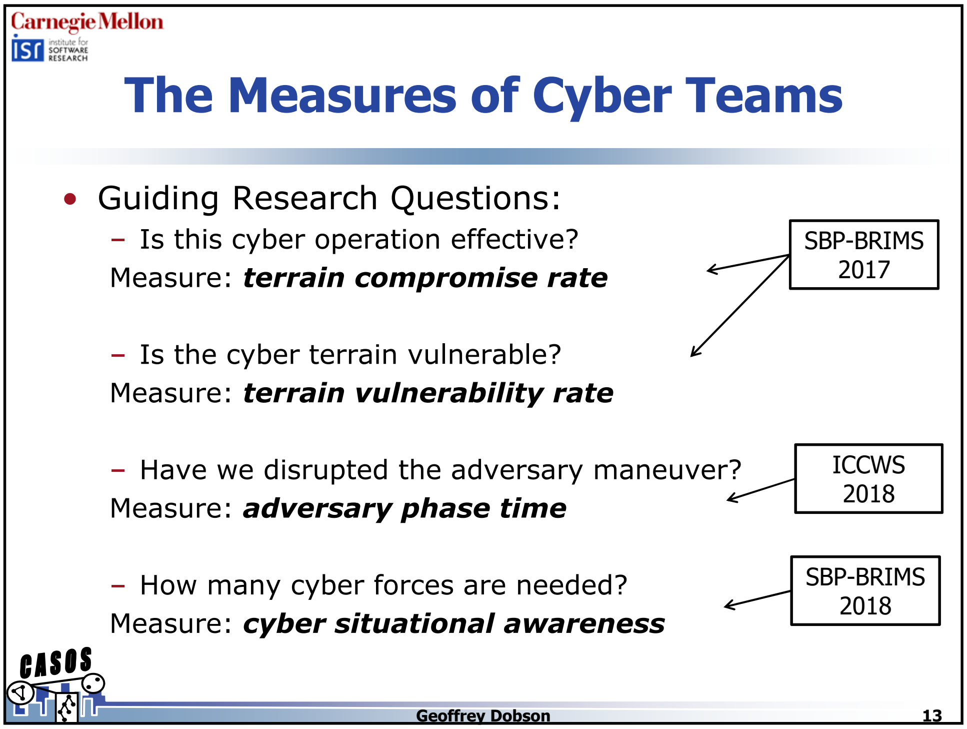


Carnegie Mellon
isr institute for SOFTWARE RESEARCH

The Measures of Cyber Teams

- Guiding Research Questions:
  - Is this cyber operation effective?
  - Is the cyber terrain vulnerable?
  - Have we disrupted the adversary maneuver?
  - How many cyber forces are necessary?

CASOS



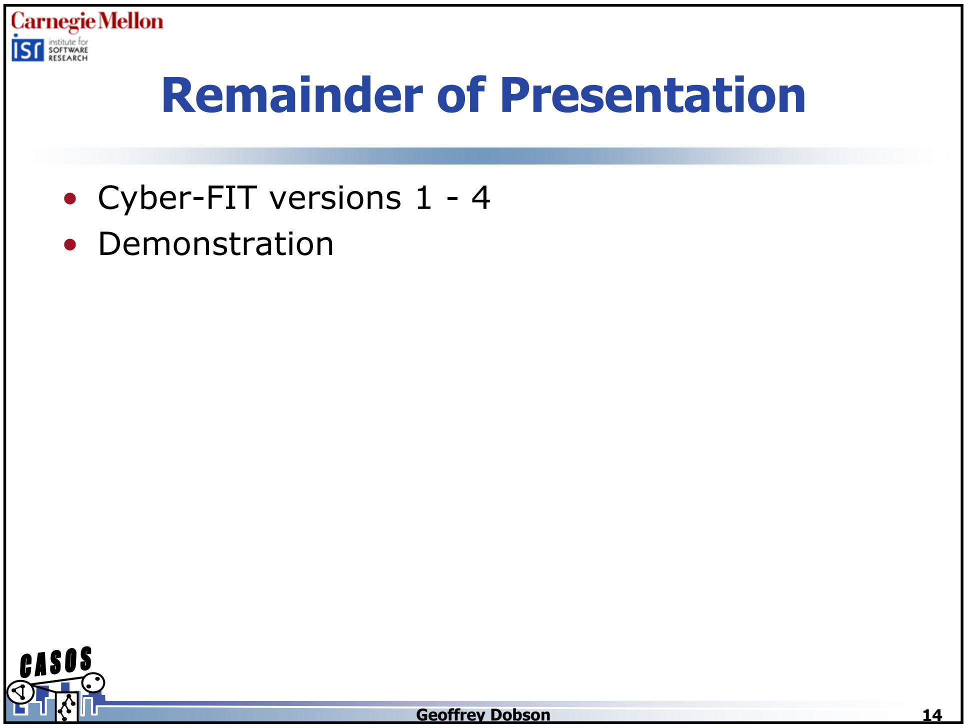
The Measures of Cyber Teams

- Guiding Research Questions:
  - Is this cyber operation effective?
    Measure: ***terrain compromise rate***
  - Is the cyber terrain vulnerable?
    Measure: ***terrain vulnerability rate***
  - Have we disrupted the adversary maneuver?
    Measure: ***adversary phase time***
  - How many cyber forces are needed?
    Measure: ***cyber situational awareness***

SBP-BRIMS 2017

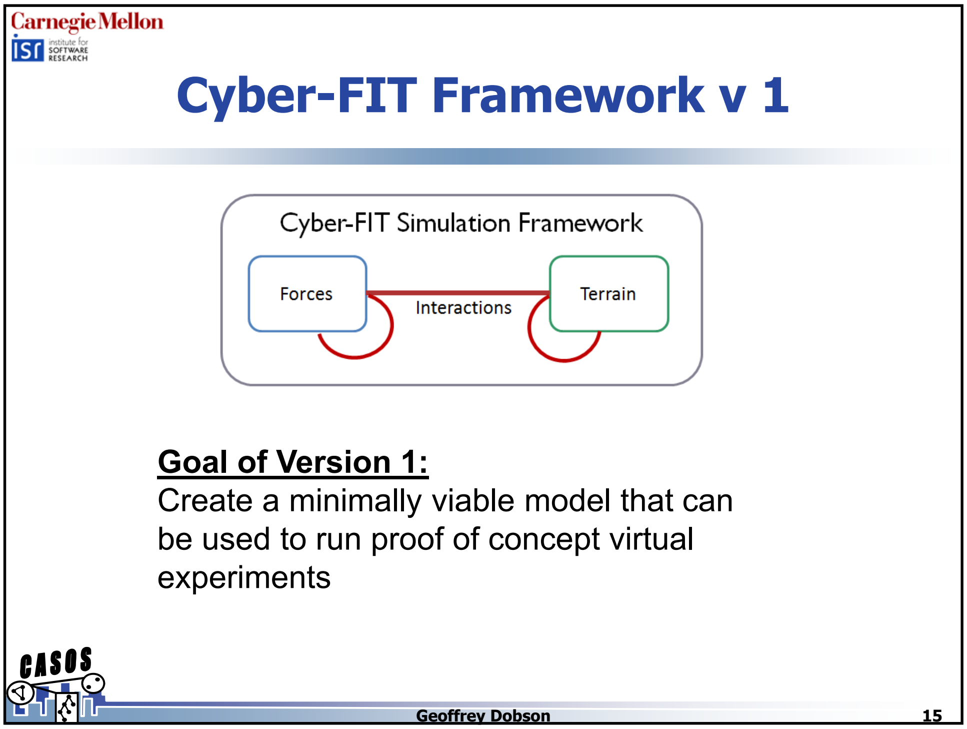
ICCWS 2018

SBP-BRIMS 2018



Remainder of Presentation

- Cyber-FIT versions 1 - 4
- Demonstration



Carnegie Mellon

isr institute for SOFTWARE RESEARCH

Cyber-FIT Framework v 1

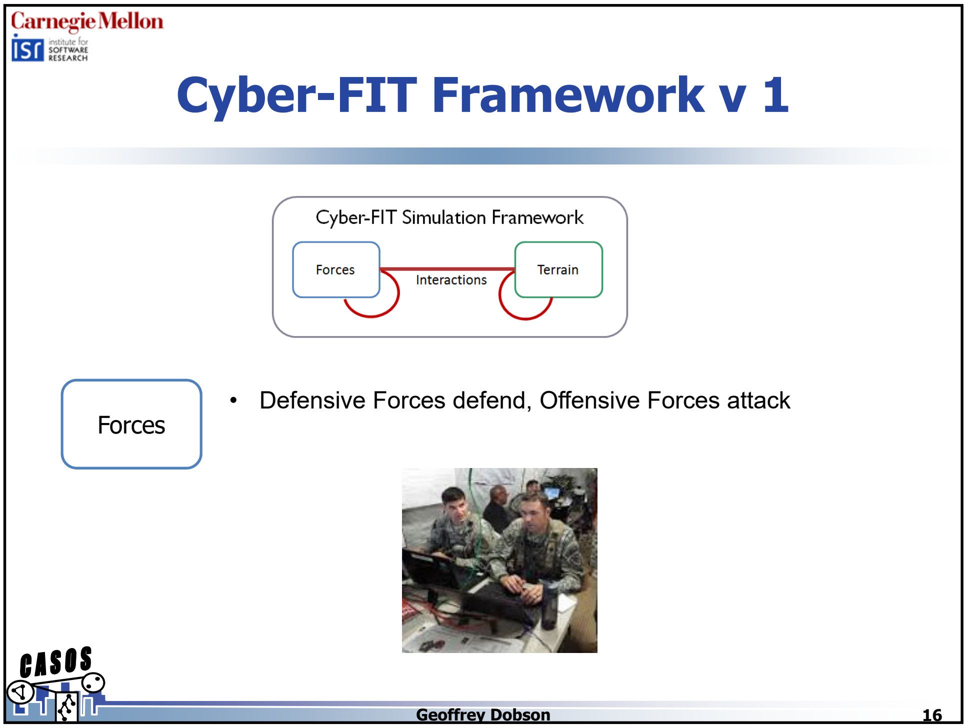
Cyber-FIT Simulation Framework

Forces

Interactions

Terrain

Goal of Version 1:
Create a minimally viable model that can be used to run proof of concept virtual experiments



Carnegie Mellon

isr institute for SOFTWARE RESEARCH

Cyber-FIT Framework v 1

Cyber-FIT Simulation Framework

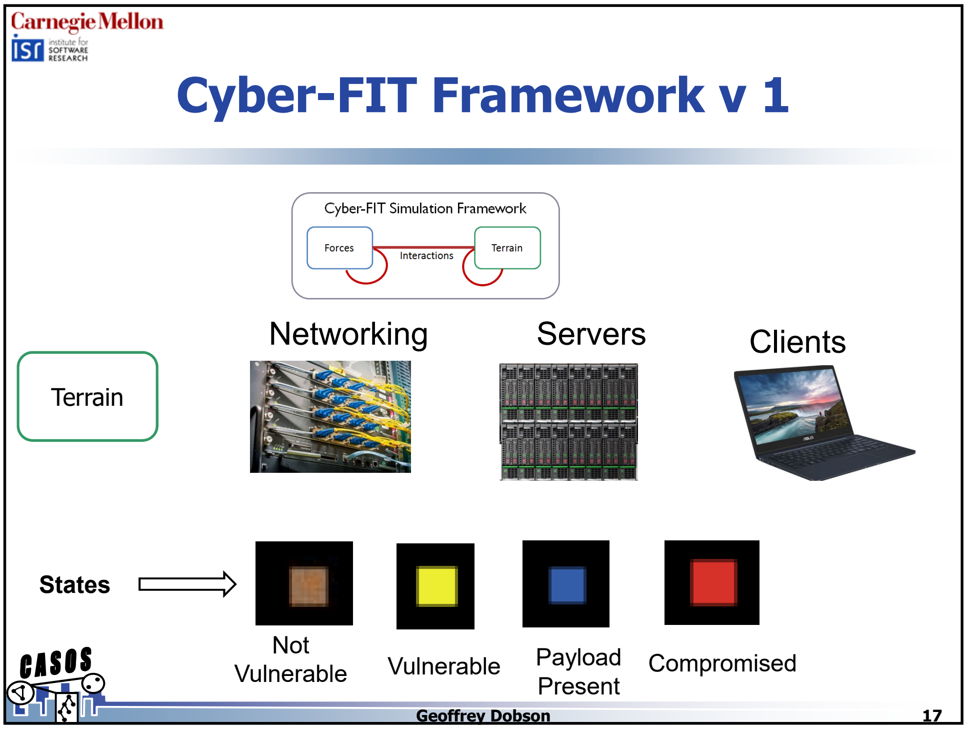
Forces

Interactions

Terrain

Forces

- Defensive Forces defend, Offensive Forces attack



Carnegie Mellon

Cyber-FIT Framework v 1

Terrain

Networking

Servers

Clients

States

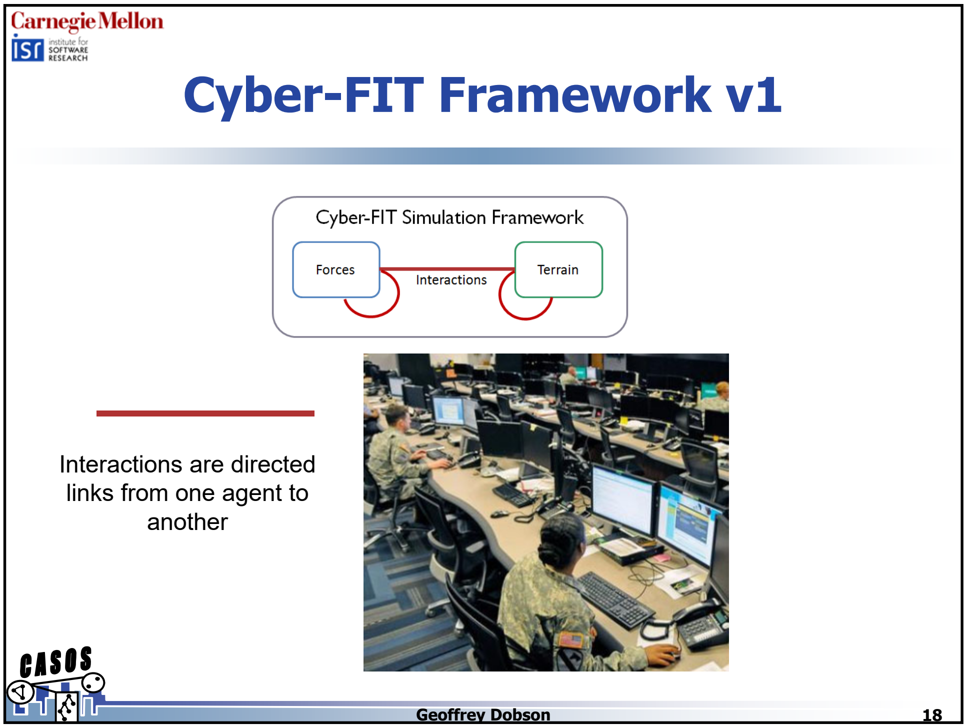
Not Vulnerable

Vulnerable

Payload Present

Compromised

Geoffrey Dobson

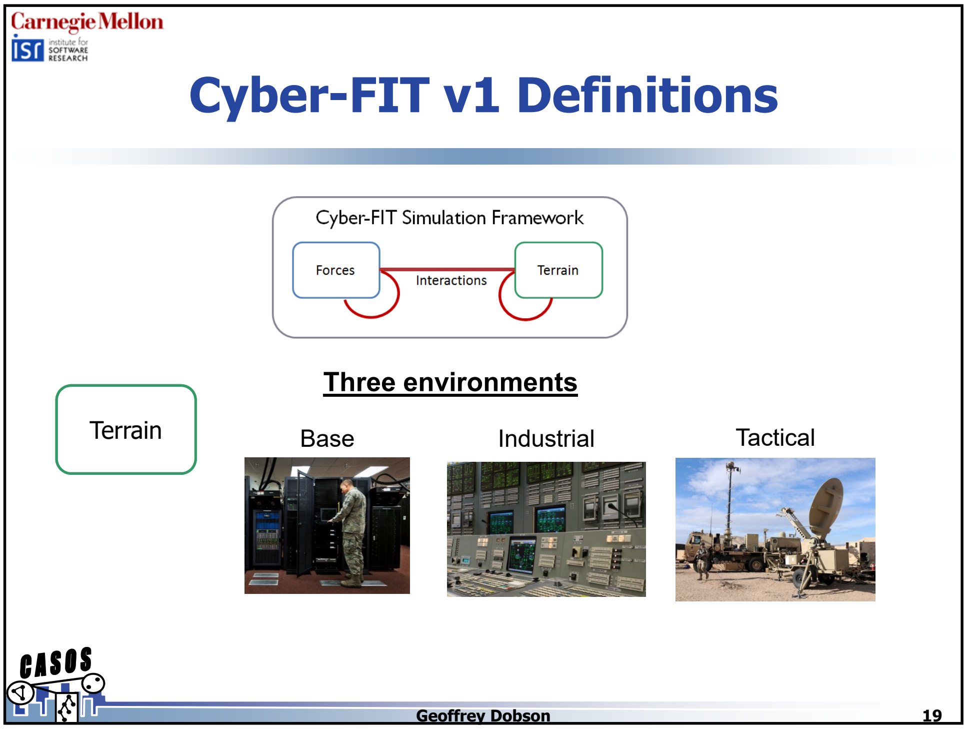


Carnegie Mellon

Cyber-FIT Framework v1

Interactions are directed links from one agent to another

Geoffrey Dobson



Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Cyber-FIT v1 Definitions

Cyber-FIT Simulation Framework

Forces — Interactions — Terrain

Terrain

Three environments

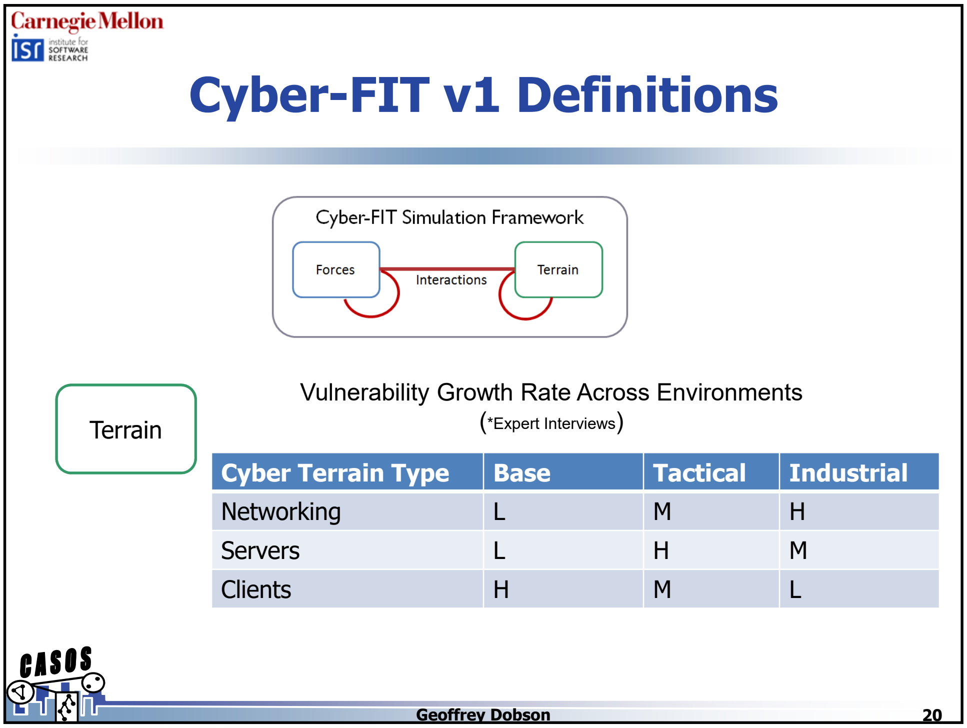
Base

Industrial

Tactical

Geoffrey Dobson

19



Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Cyber-FIT v1 Definitions

Cyber-FIT Simulation Framework

Forces — Interactions — Terrain

Terrain

Vulnerability Growth Rate Across Environments
(*Expert Interviews)

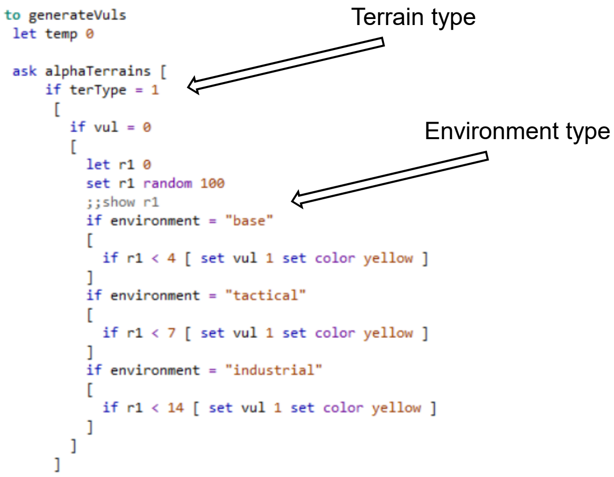
Cyber Terrain Type	Base	Tactical	Industrial
Networking	L	M	H
Servers	L	H	M
Clients	H	M	L

Geoffrey Dobson

20

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Cyber-FIT v1 Definitions



```
to generateVuls
 let temp 0

 ask alphaTerrains [
     if terType = 1
     [
       if vul = 0
       [
         let r1 0
         set r1 random 100
         ;;show r1
         if environment = "base"
         [
           if r1 < 4 [ set vul 1 set color yellow ]
         ]
         if environment = "tactical"
         [
           if r1 < 7 [ set vul 1 set color yellow ]
         ]
         if environment = "industrial"
         [
           if r1 < 14 [ set vul 1 set color yellow ]
         ]
       ]
     ]
```

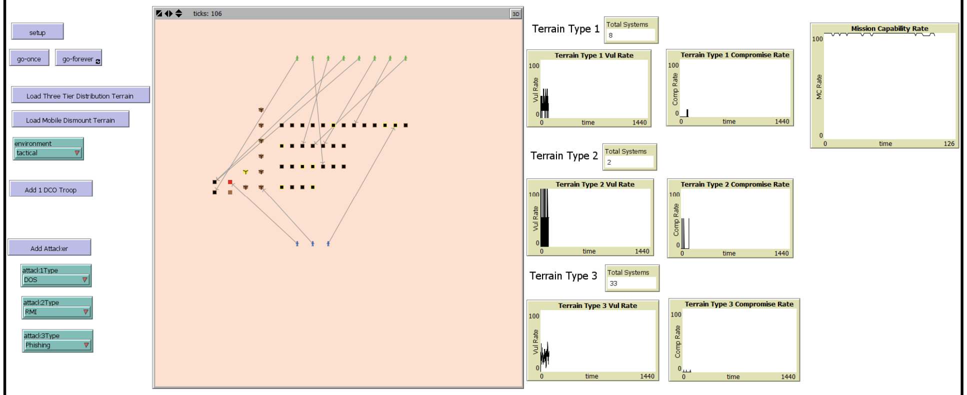
Terrain type

Environment type

CASOS

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Cyber-FIT v 1



ticks: 106

environment: tactical

attack1Type: DOS

attack2Type: RMI

attack3Type: Phishing

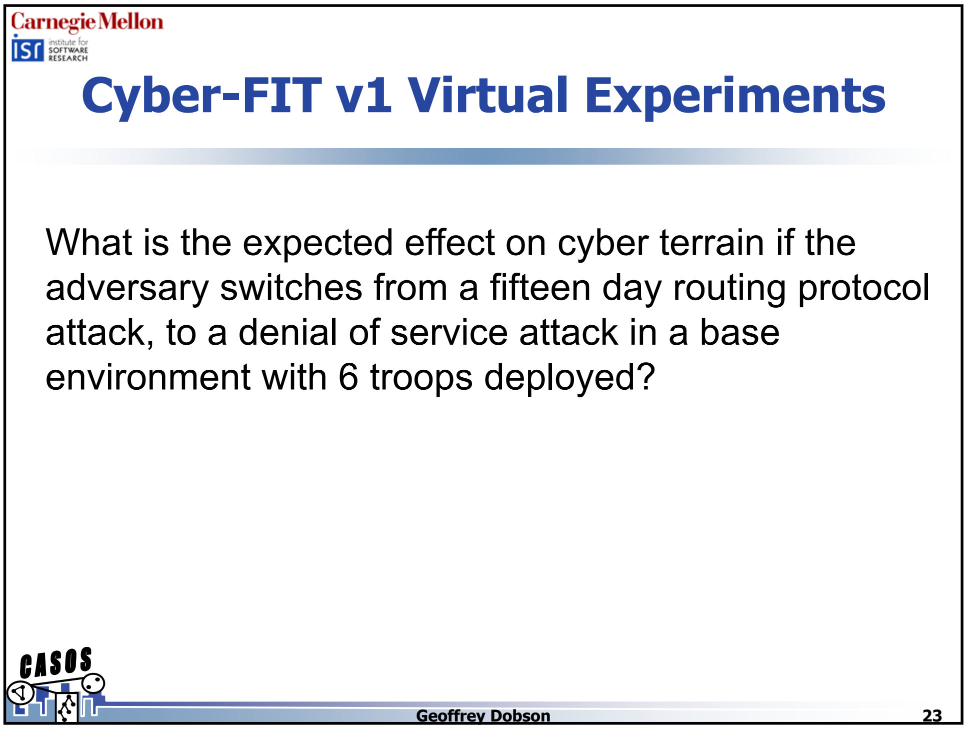
Terrain Type 1 Total Systems 8

Terrain Type 2 Total Systems 2

Terrain Type 3 Total Systems 33

CASOS

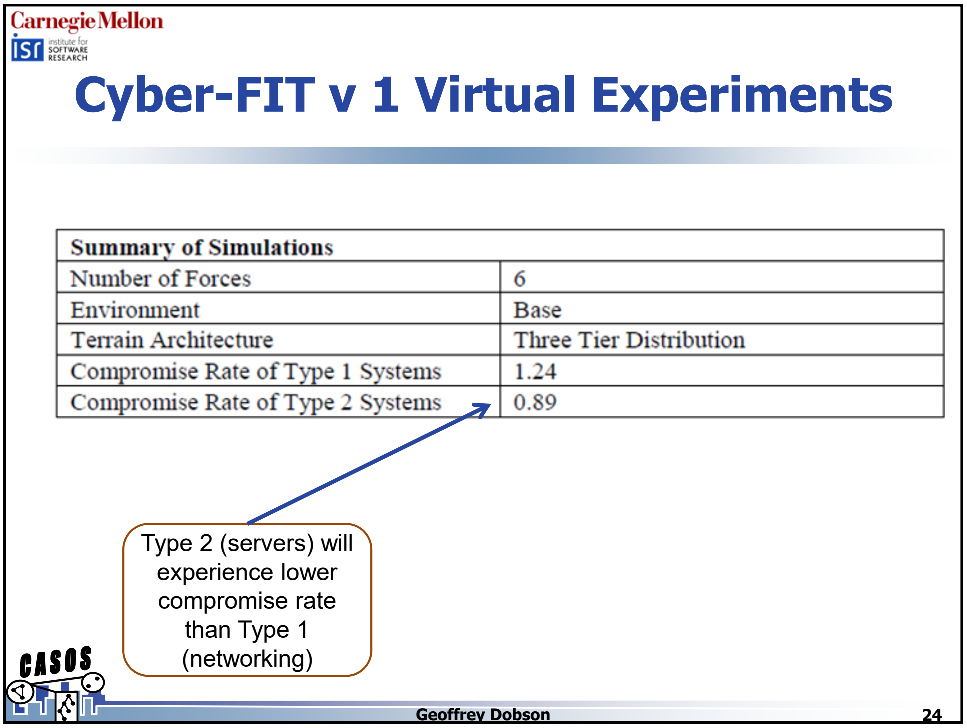
CASOS



Carnegie Mellon

Cyber-FIT v1 Virtual Experiments

What is the expected effect on cyber terrain if the adversary switches from a fifteen day routing protocol attack, to a denial of service attack in a base environment with 6 troops deployed?



Carnegie Mellon

Cyber-FIT v 1 Virtual Experiments

Summary of Simulations	
Number of Forces	6
Environment	Base
Terrain Architecture	Three Tier Distribution
Compromise Rate of Type 1 Systems	1.24
Compromise Rate of Type 2 Systems	0.89

Type 2 (servers) will experience lower compromise rate than Type 1 (networking)

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Cyber-FIT v1

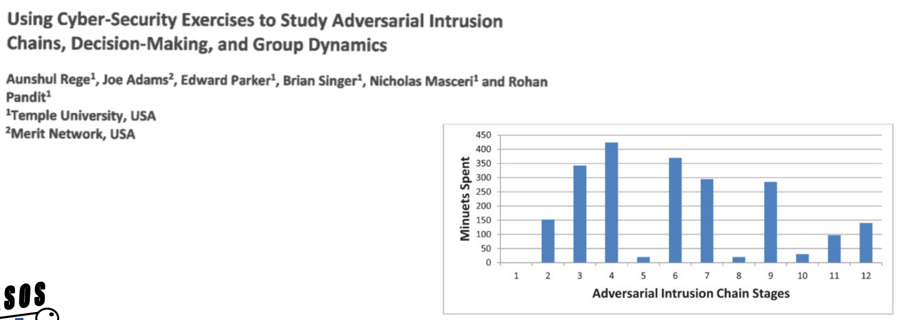
Goal of Version 1:
Create a minimally viable model that can be used to run proof of concept virtual experiments

✓

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Cyber-FIT v2

Goal of Version 2:
Incorporate empirical data to add realistic complexity to the model

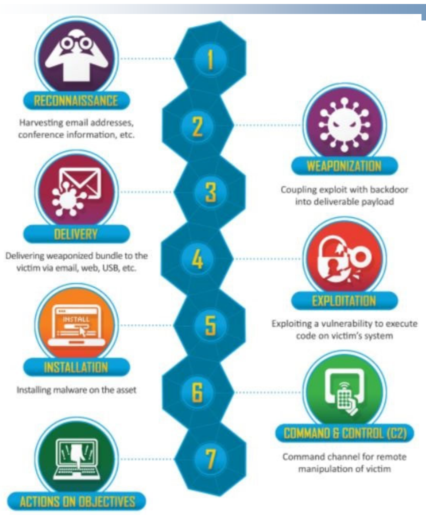


Using Cyber-Security Exercises to Study Adversarial Intrusion Chains, Decision-Making, and Group Dynamics

Aunshul Rege[1], Joe Adams[2], Edward Parker[1], Brian Singer[1], Nicholas Masceri[1] and Rohan Pandit[1]
[1]Temple University, USA
[2]Merit Network, USA

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Cyber-FIT v2

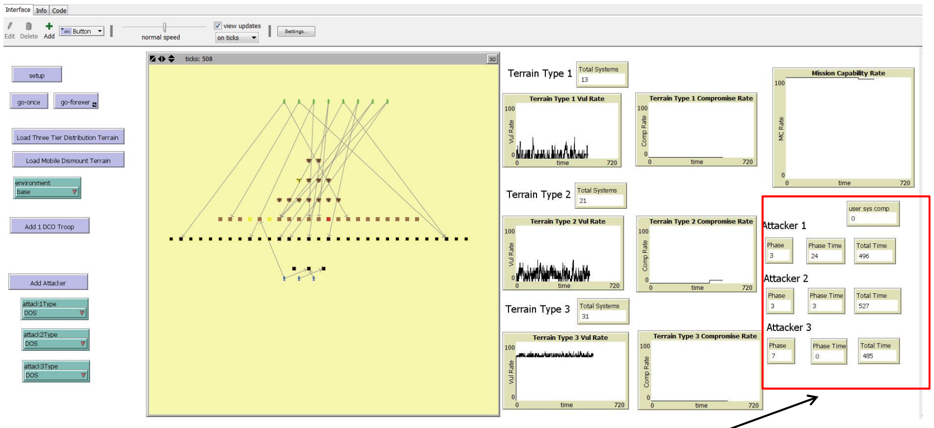

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES

Force the attacker agents to traverse the cyber kill chain

Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Cyber-FIT v2



☑ view updates

ticks: 508

environment: base

attack1Type: DOS

attack2Type: DOS

attack3Type: DOS

Terrain Type 1 — Total Systems: 13

Terrain Type 2 — Total Systems: 21

Terrain Type 3 — Total Systems: 31

user sys comp: 0

Attacker 1 — Phase: 3, Phase Time: 24, Total Time: 496

Attacker 2 — Phase: 3, Phase Time: 3, Total Time: 527

Attacker 3 — Phase: 7, Phase Time: 0, Total Time: 485

Adversary Behavior Modeling

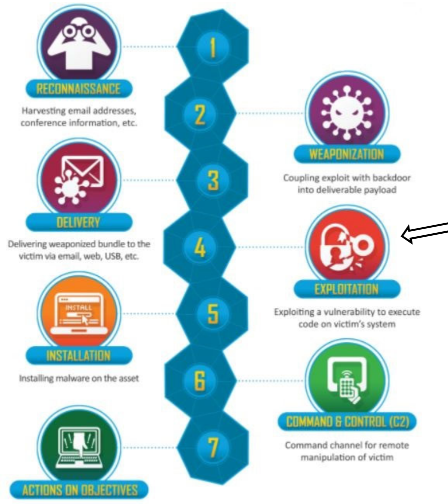
Cyber-FIT v2 Virtual Experiments

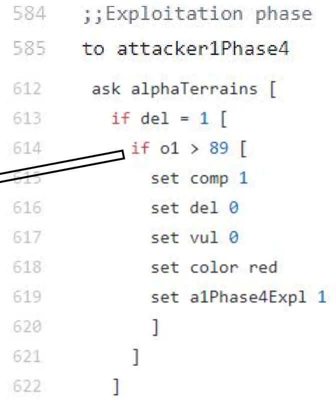
What is expected time to complete phases three and four during a denial of service attack, with six defensive cyber forces deployed, as the exploitation success rate is increased from two to forty?

How to decrease exploit success rate?

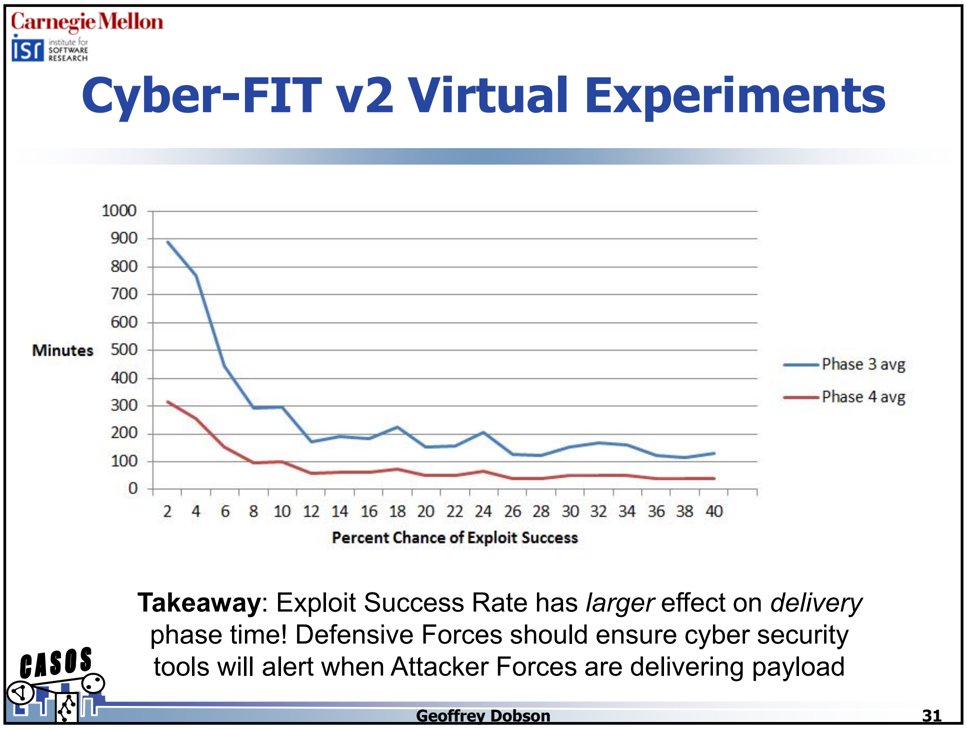
- Updated Operating Systems and Software
- Patching
- Maintenance
- User Access Control
- Training

Cyber-FIT v2 Virtual Experiments


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES



```
;;Exploitation phase
to attacker1Phase4
 ask alphaTerrains [
   if del = 1 [
     if o1 > 89 [
       set comp 1
       set del 0
       set vul 0
       set color red
       set a1Phase4Expl 1
       ]
     ]
   ]
```

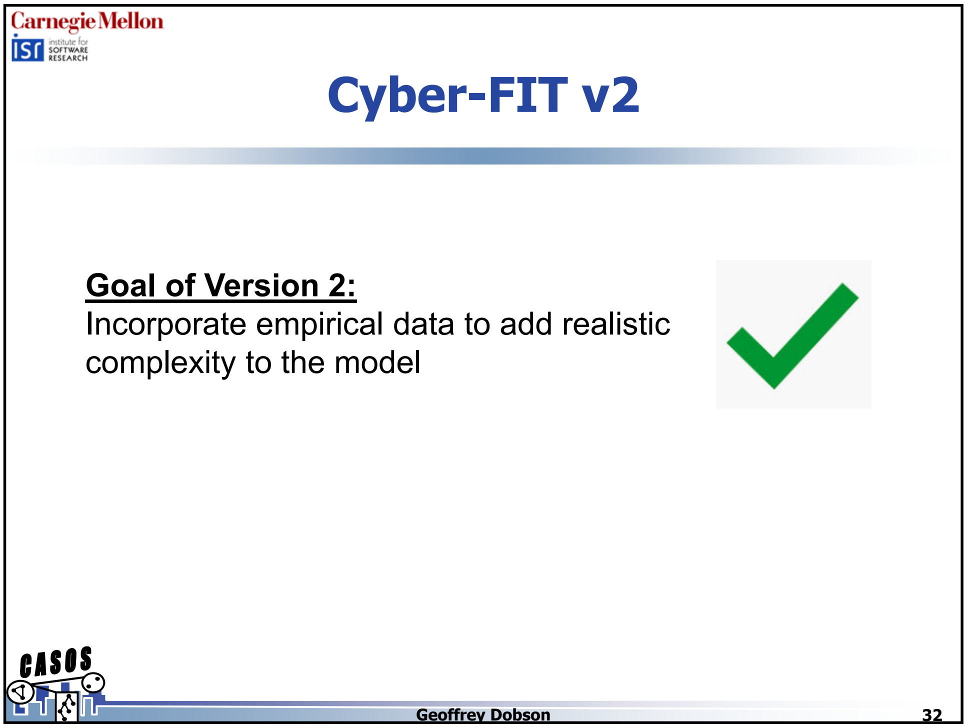


Carnegie Mellon isr institute for SOFTWARE RESEARCH

Cyber-FIT v2 Virtual Experiments

Takeaway: Exploit Success Rate has *larger* effect on *delivery* phase time! Defensive Forces should ensure cyber security tools will alert when Attacker Forces are delivering payload

CASOS

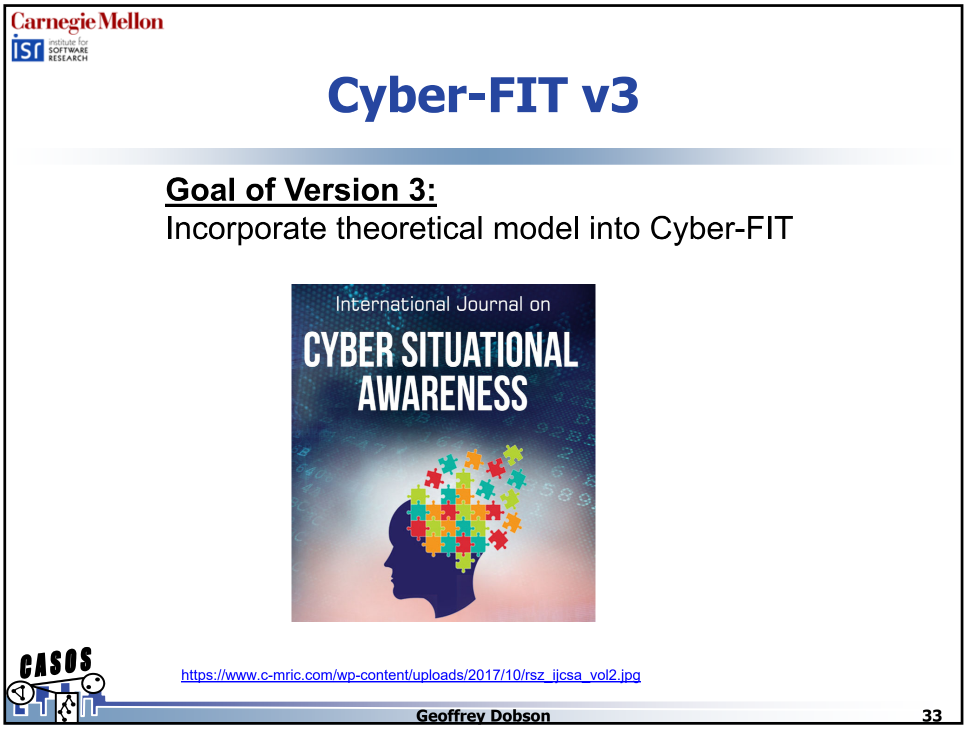


Carnegie Mellon isr institute for SOFTWARE RESEARCH

Cyber-FIT v2

Goal of Version 2:
Incorporate empirical data to add realistic complexity to the model ✓

CASOS



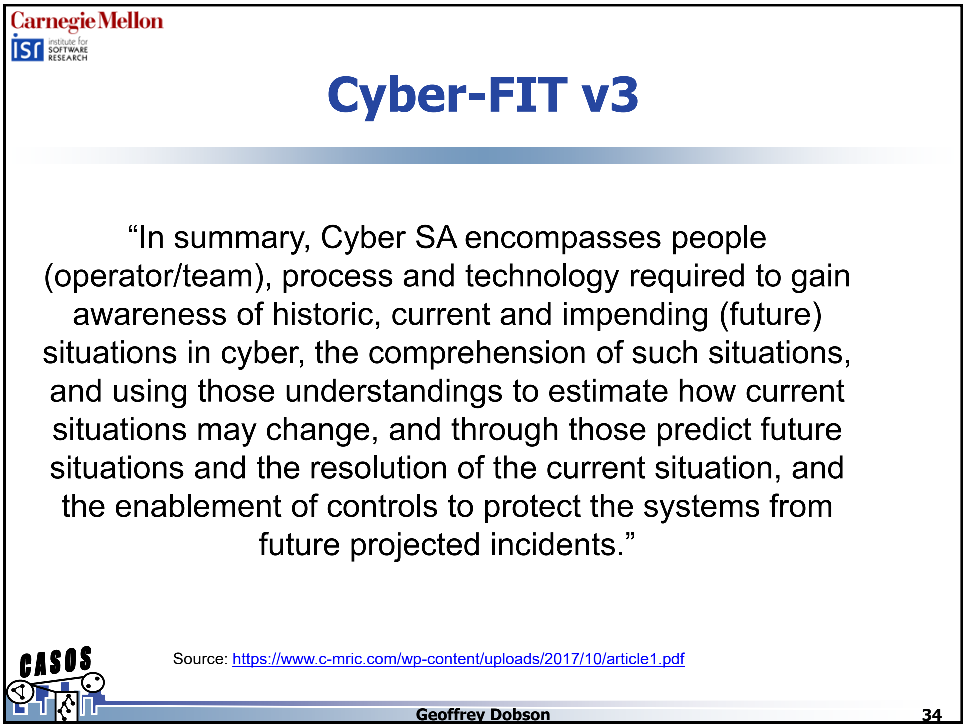
Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Cyber-FIT v3

Goal of Version 3:
Incorporate theoretical model into Cyber-FIT

International Journal on
CYBER SITUATIONAL AWARENESS

https://www.c-mric.com/wp-content/uploads/2017/10/rsz_ijcsa_vol2.jpg

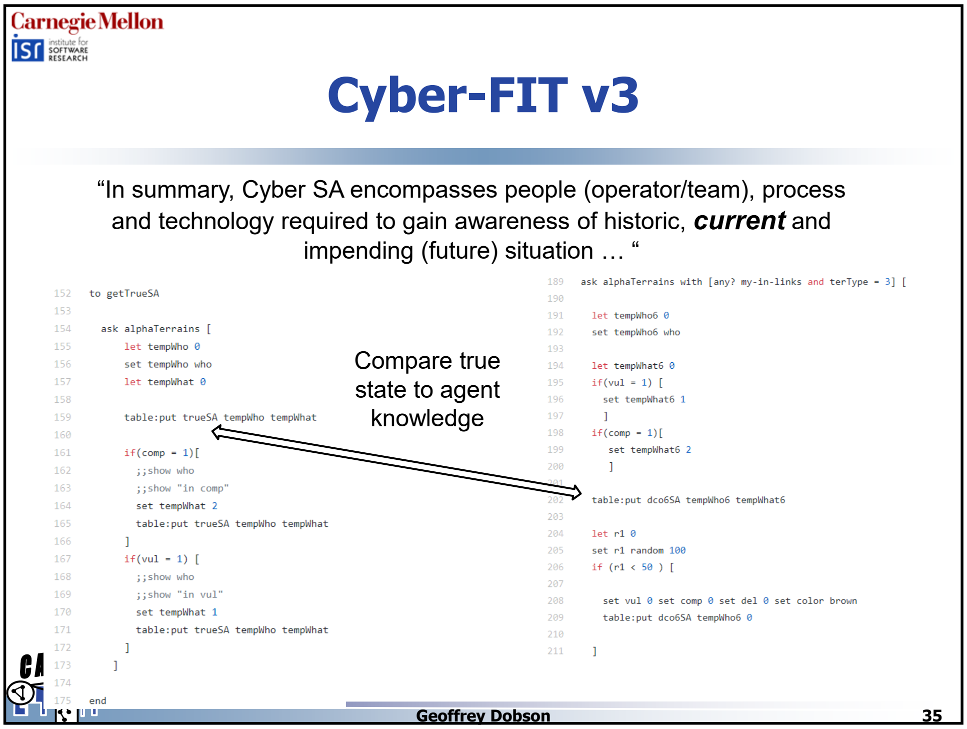


Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Cyber-FIT v3

“In summary, Cyber SA encompasses people (operator/team), process and technology required to gain awareness of historic, current and impending (future) situations in cyber, the comprehension of such situations, and using those understandings to estimate how current situations may change, and through those predict future situations and the resolution of the current situation, and the enablement of controls to protect the systems from future projected incidents.”

Source: https://www.c-mric.com/wp-content/uploads/2017/10/article1.pdf



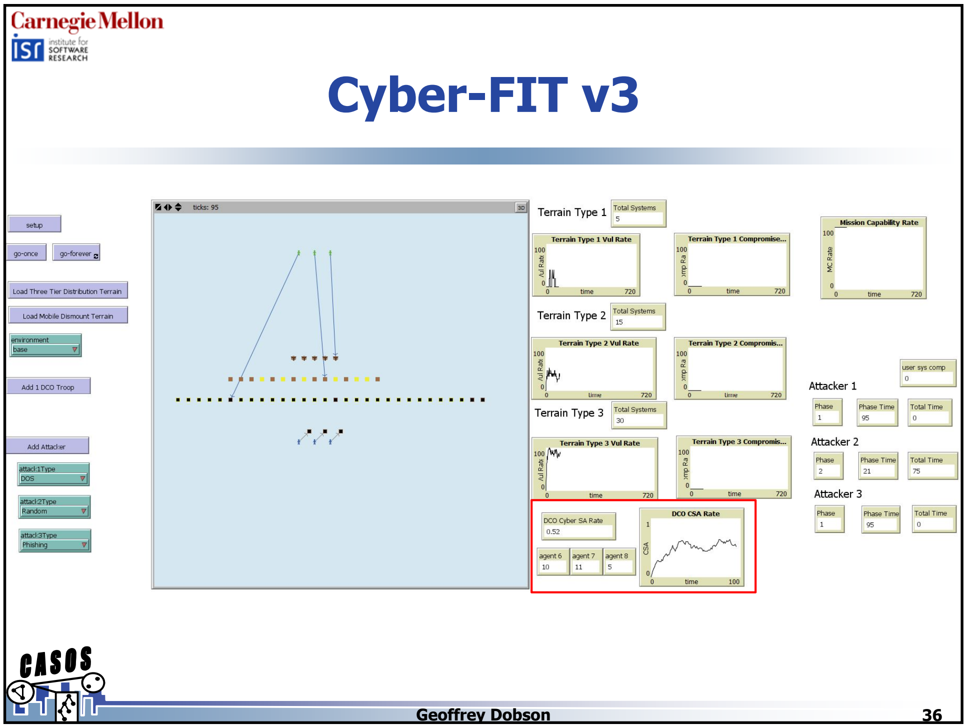
Cyber-FIT v3

“In summary, Cyber SA encompasses people (operator/team), process and technology required to gain awareness of historic, ***current*** and impending (future) situation … “

```
to getTrueSA

  ask alphaTerrains [
    let tempWho 0
    set tempWho who
    let tempWhat 0

    table:put trueSA tempWho tempWhat

    if(comp = 1)[
      ;;show who
      ;;show "in comp"
      set tempWhat 2
      table:put trueSA tempWho tempWhat
    ]
    if(vul = 1) [
      ;;show who
      ;;show "in vul"
      set tempWhat 1
      table:put trueSA tempWho tempWhat
    ]
  ]

end
```

Compare true state to agent knowledge

```
ask alphaTerrains with [any? my-in-links and terType = 3] [

  let tempWho6 0
  set tempWho6 who

  let tempWhat6 0
  if(vul = 1) [
    set tempWhat6 1
    ]
  if(comp = 1)[
     set tempWhat6 2
     ]

  table:put dco6SA tempWho6 tempWhat6

  let r1 0
  set r1 random 100
  if (r1 < 50 ) [

    set vul 0 set comp 0 set del 0 set color brown
    table:put dco6SA tempWho6 0

  ]
```



Cyber-FIT v3

environment: base

attack1Type: DOS

attack2Type: Random

attack3Type: Phishing

Terrain Type 1 — Total Systems: 5

Terrain Type 2 — Total Systems: 15

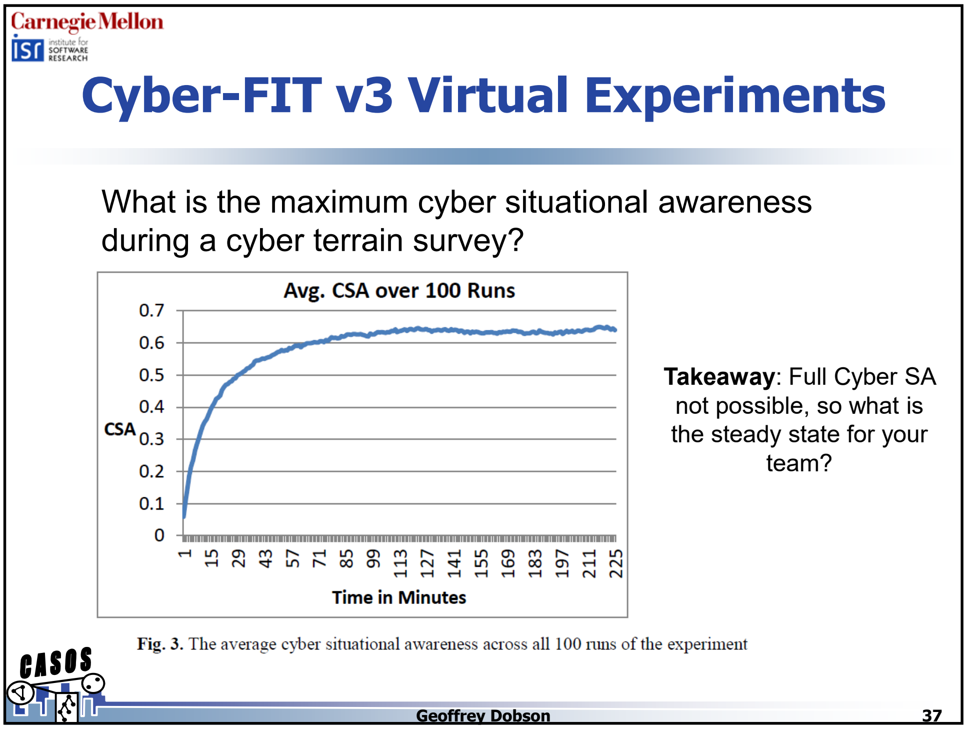
Terrain Type 3 — Total Systems: 30

DCO Cyber SA Rate: 0.52

agent 6	agent 7	agent 8
10	11	5

user sys comp: 0

	Phase	Phase Time	Total Time
Attacker 1	1	95	0
Attacker 2	2	21	75
Attacker 3	1	95	0



Carnegie Mellon

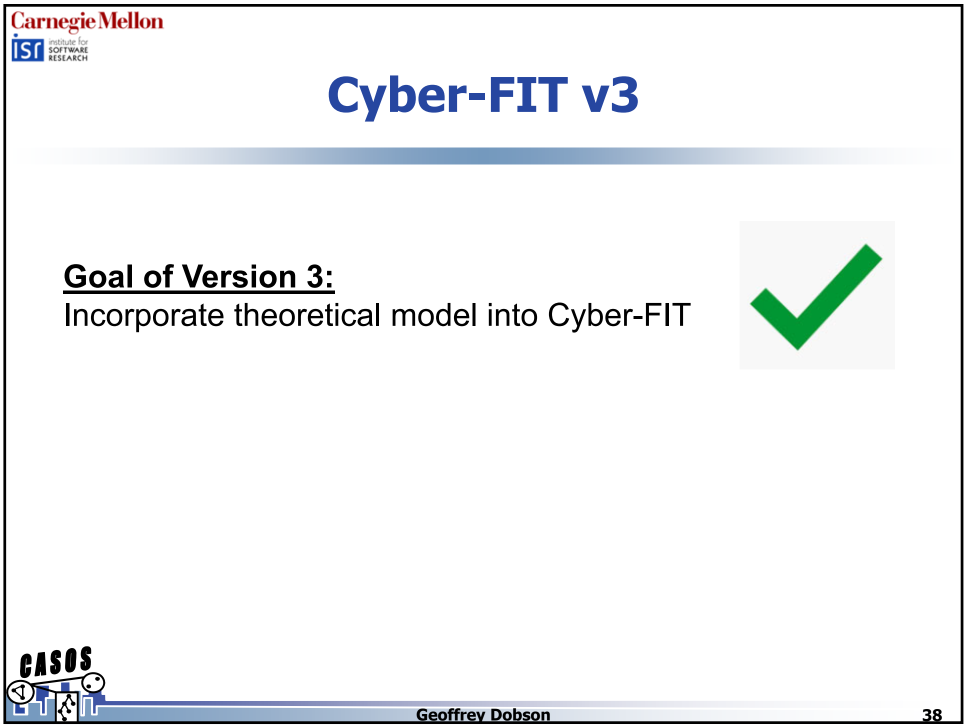
Cyber-FIT v3 Virtual Experiments

What is the maximum cyber situational awareness during a cyber terrain survey?

Takeaway: Full Cyber SA not possible, so what is the steady state for your team?

Fig. 3. The average cyber situational awareness across all 100 runs of the experiment

Geoffrey Dobson 37



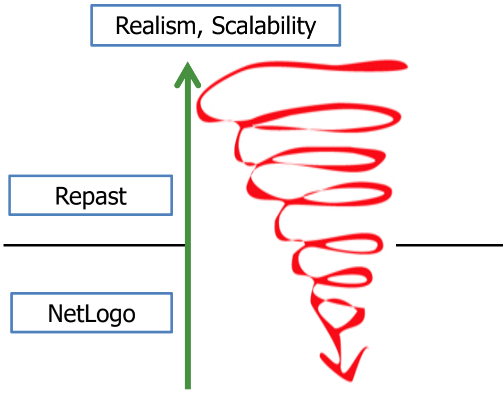
Carnegie Mellon

Cyber-FIT v3

Goal of Version 3:
Incorporate theoretical model into Cyber-FIT ✓

Geoffrey Dobson 38

Cyber-FIT Spiral Development



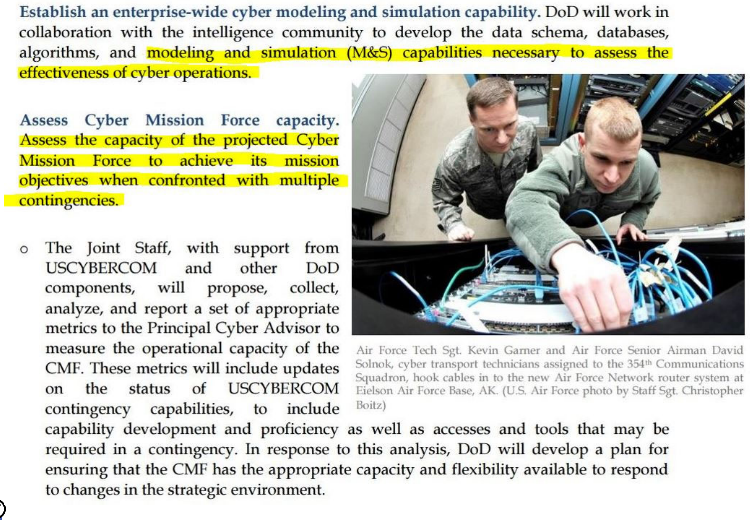
Realism, Scalability

Repast

NetLogo

V5	TBD
V4	The Performance Measures of Cyber Teams
V3	Explored Cyber Situational Awareness Theory
V2	Added Empirical Data
V1	Foundation

The Performance Measures of Cyber Teams

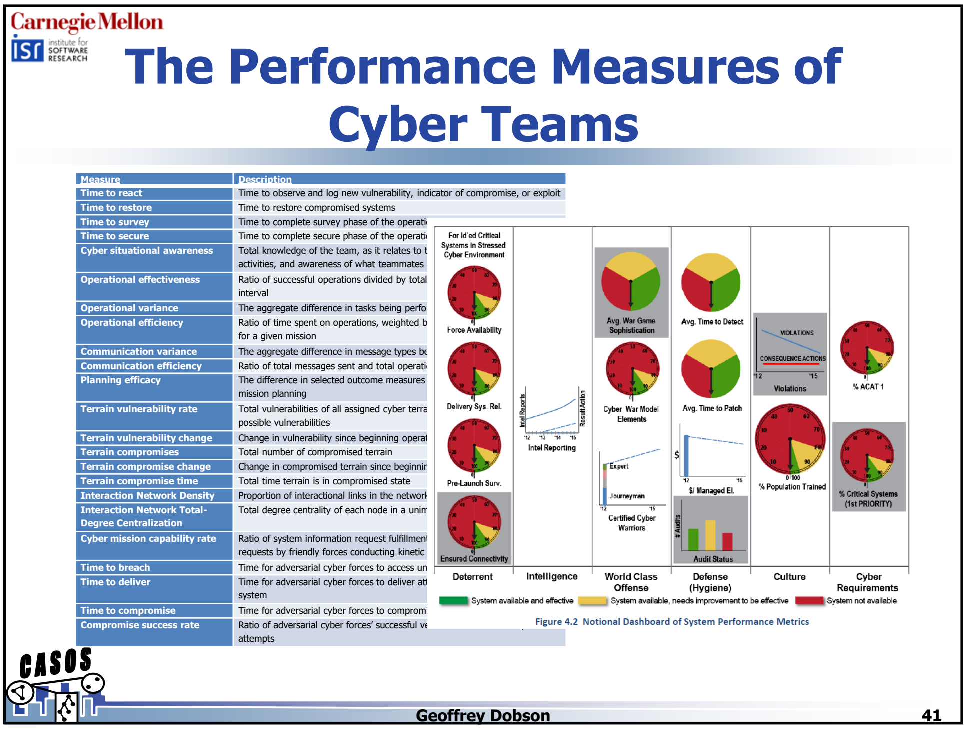


Establish an enterprise-wide cyber modeling and simulation capability. DoD will work in collaboration with the intelligence community to develop the data schema, databases, algorithms, and modeling and simulation (M&S) capabilities necessary to assess the effectiveness of cyber operations.

Assess Cyber Mission Force capacity. Assess the capacity of the projected Cyber Mission Force to achieve its mission objectives when confronted with multiple contingencies.

- The Joint Staff, with support from USCYBERCOM and other DoD components, will propose, collect, analyze, and report a set of appropriate metrics to the Principal Cyber Advisor to measure the operational capacity of the CMF. These metrics will include updates on the status of USCYBERCOM contingency capabilities, to include capability development and proficiency as well as accesses and tools that may be required in a contingency. In response to this analysis, DoD will develop a plan for ensuring that the CMF has the appropriate capacity and flexibility available to respond to changes in the strategic environment.

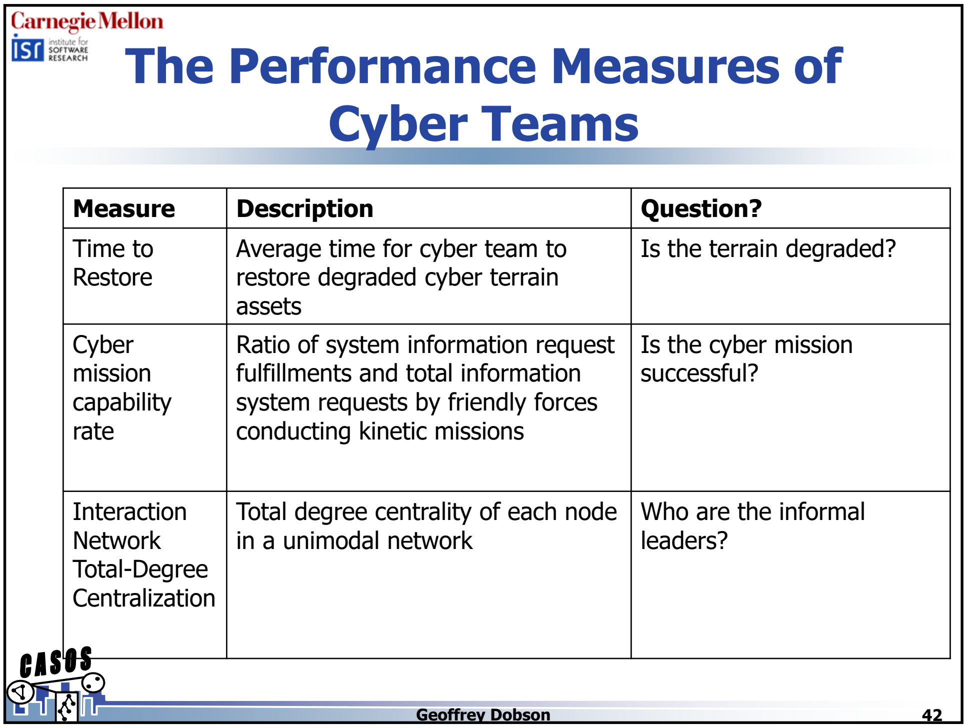
Air Force Tech Sgt. Kevin Garner and Air Force Senior Airman David Solnok, cyber transport technicians assigned to the 354th Communications Squadron, hook cables in to the new Air Force Network router system at Eielson Air Force Base, AK. (U.S. Air Force photo by Staff Sgt. Christopher Boitz)



The Performance Measures of Cyber Teams

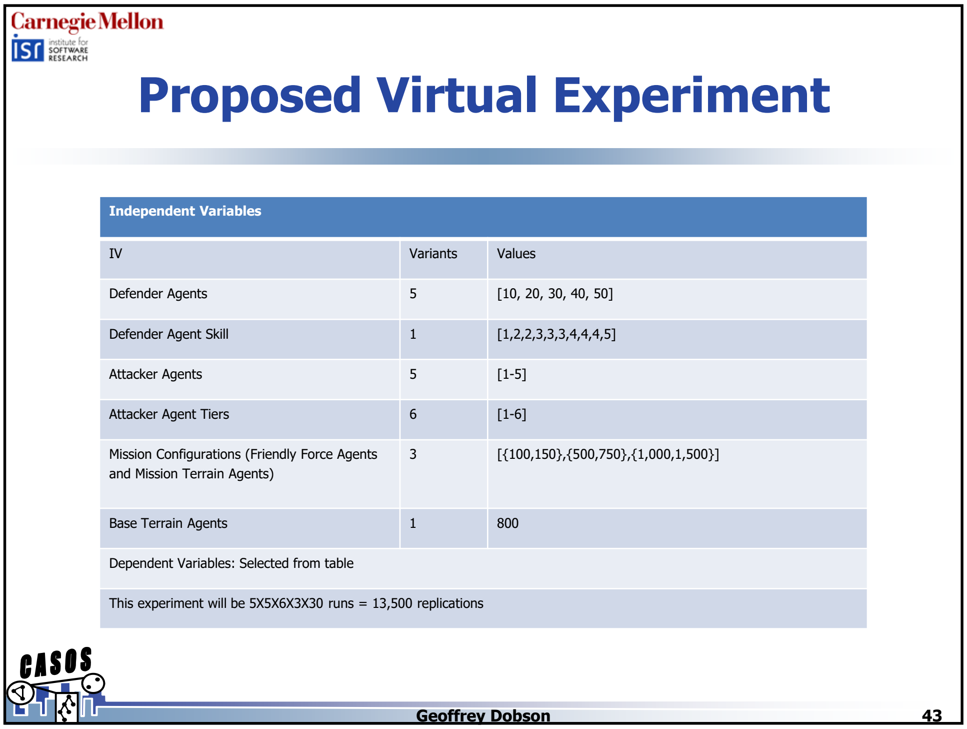
Measure	Description
Time to react	Time to observe and log new vulnerability, indicator of compromise, or exploit
Time to restore	Time to restore compromised systems
Time to survey	Time to complete survey phase of the operati
Time to secure	Time to complete secure phase of the operati
Cyber situational awareness	Total knowledge of the team, as it relates to t activities, and awareness of what teammates
Operational effectiveness	Ratio of successful operations divided by total interval
Operational variance	The aggregate difference in tasks being perfo
Operational efficiency	Ratio of time spent on operations, weighted b for a given mission
Communication variance	The aggregate difference in message types be
Communication efficiency	Ratio of total messages sent and total operati
Planning efficacy	The difference in selected outcome measures mission planning
Terrain vulnerability rate	Total vulnerabilities of all assigned cyber terra possible vulnerabilities
Terrain vulnerability change	Change in vulnerability since beginning operat
Terrain compromises	Total number of compromised terrain
Terrain compromise change	Change in compromised terrain since beginnir
Terrain compromise time	Total time terrain is in compromised state
Interaction Network Density	Proportion of interactional links in the network
Interaction Network Total-Degree Centralization	Total degree centrality of each node in a unim
Cyber mission capability rate	Ratio of system information request fulfillment requests by friendly forces conducting kinetic
Time to breach	Time for adversarial cyber forces to access un
Time to deliver	Time for adversarial cyber forces to deliver att system
Time to compromise	Time for adversarial cyber forces to compromi
Compromise success rate	Ratio of adversarial cyber forces' successful ve attempts

Figure 4.2 Notional Dashboard of System Performance Metrics



The Performance Measures of Cyber Teams

Measure	Description	Question?
Time to Restore	Average time for cyber team to restore degraded cyber terrain assets	Is the terrain degraded?
Cyber mission capability rate	Ratio of system information request fulfillments and total information system requests by friendly forces conducting kinetic missions	Is the cyber mission successful?
Interaction Network Total-Degree Centralization	Total degree centrality of each node in a unimodal network	Who are the informal leaders?

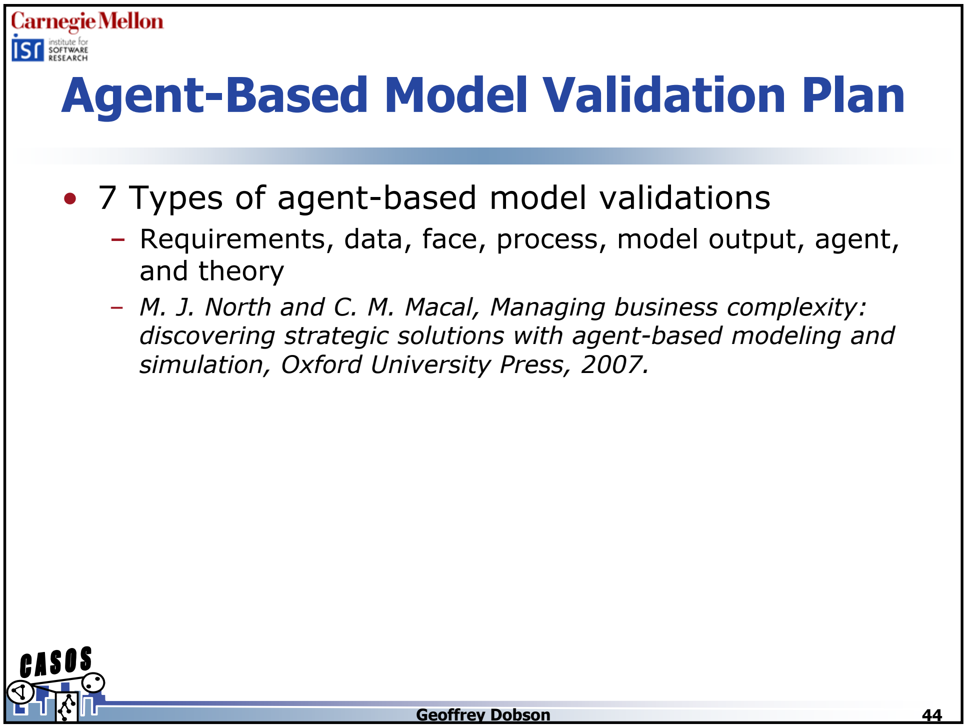


Carnegie Mellon

isr institute for SOFTWARE RESEARCH

Proposed Virtual Experiment

Independent Variables		
IV	Variants	Values
Defender Agents	5	[10, 20, 30, 40, 50]
Defender Agent Skill	1	[1,2,2,3,3,3,4,4,4,5]
Attacker Agents	5	[1-5]
Attacker Agent Tiers	6	[1-6]
Mission Configurations (Friendly Force Agents and Mission Terrain Agents)	3	[{100,150},{500,750},{1,000,1,500}]
Base Terrain Agents	1	800
Dependent Variables: Selected from table		
This experiment will be 5X5X6X3X30 runs = 13,500 replications		



Carnegie Mellon

isr institute for SOFTWARE RESEARCH

Agent-Based Model Validation Plan

- 7 Types of agent-based model validations
  - Requirements, data, face, process, model output, agent, and theory
  - *M. J. North and C. M. Macal, Managing business complexity: discovering strategic solutions with agent-based modeling and simulation, Oxford University Press, 2007.*

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Model Validation Plan

1. Requirements Validation

<u>Guiding Question</u>:

Is this model solving the right problem?

Discuss with a focus group of military planners and strategists

CASOS

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

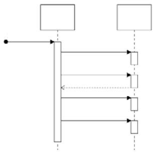
Model Validation Plan

2. Data Validation

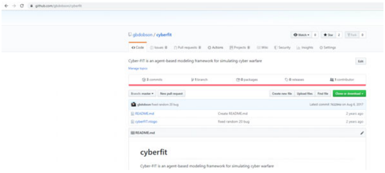
<u>Guiding Question</u>:

Has the data used in the model been validated?

UML



Source code on Github



github.com/gbdobson/cyberfit

gbdobson / cyberfit

Watch 0 Star 2 Fork 0

Code Issues 0 Pull requests 0 Actions Projects 0 Wiki Security Insights Settings

Cyber-FIT is an agent-based modeling framework for simulating cyber warfare

Manage topics

3 commits 1 branch 0 packages 0 releases 1 contributor

Branch: master New pull request Create new file Upload files Find file Clone or download

gbdobson fixed random 20 bug Latest commit 7622844 on Aug 6, 2017

README.md	Create README.md	2 years ago
cyberFIT.nlogo	fixed random 20 bug	2 years ago

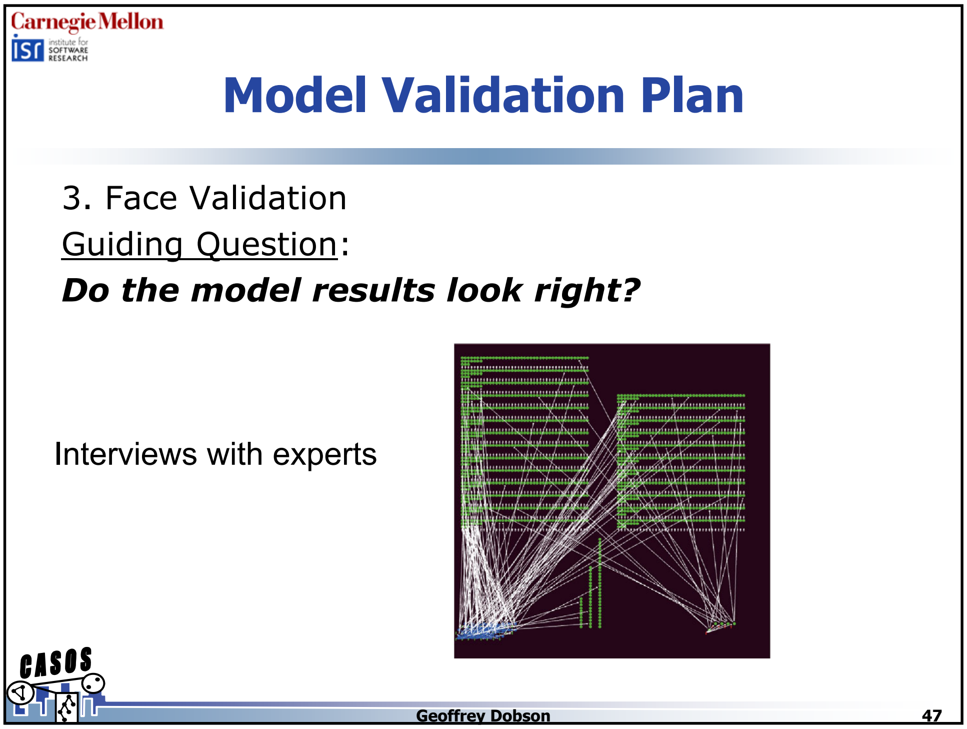
README.md

cyberfit

Cyber-FIT is an agent-based modeling framework for simulating cyber warfare

CASOS

CASOS



Carnegie Mellon
isr institute for SOFTWARE RESEARCH

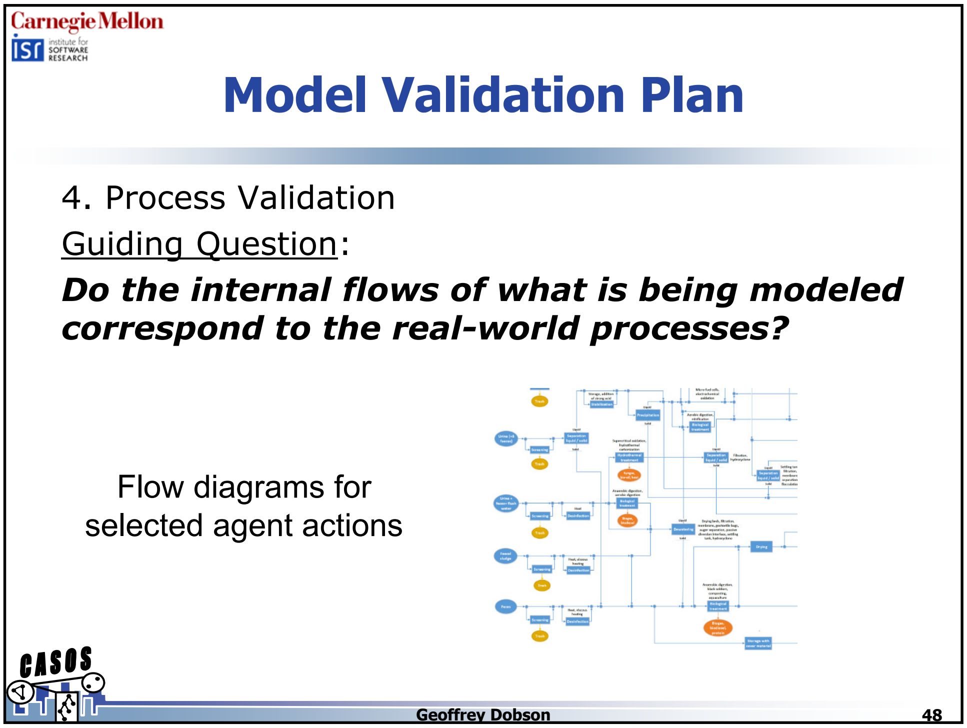
Model Validation Plan

3. Face Validation

Guiding Question:

Do the model results look right?

Interviews with experts



Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Model Validation Plan

4. Process Validation

Guiding Question:

Do the internal flows of what is being modeled correspond to the real-world processes?

Flow diagrams for selected agent actions

Carnegie Mellon

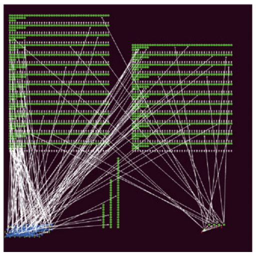
isr institute for SOFTWARE RESEARCH

Model Validation Plan

5. Model Output Validation

Guiding Question:

Do the model outputs match the outputs of real-world systems?



=

Interviews with Experts

Carnegie Mellon

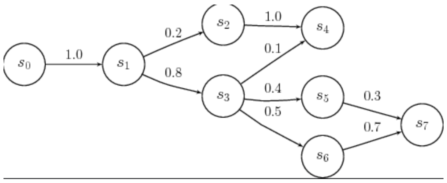
isr institute for SOFTWARE RESEARCH

Model Validation Plan

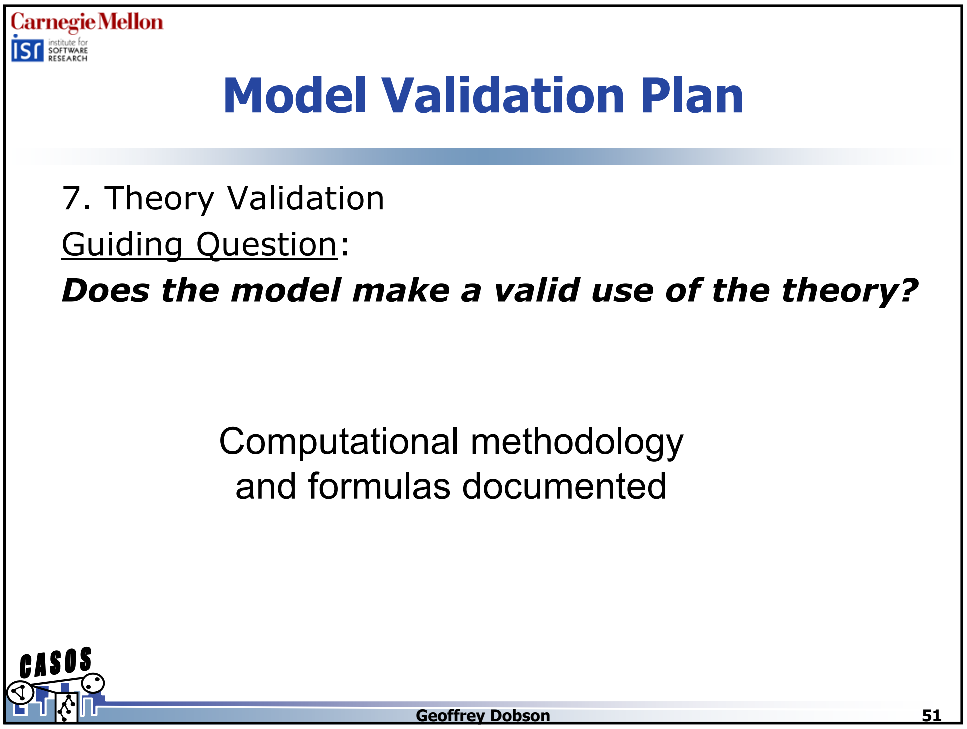
6. Agent Validation

Guiding Question:

Do agent behaviors and interaction mechanisms correspond to agents in the real world?



Markov Chains for selected agent types compared against real world data *



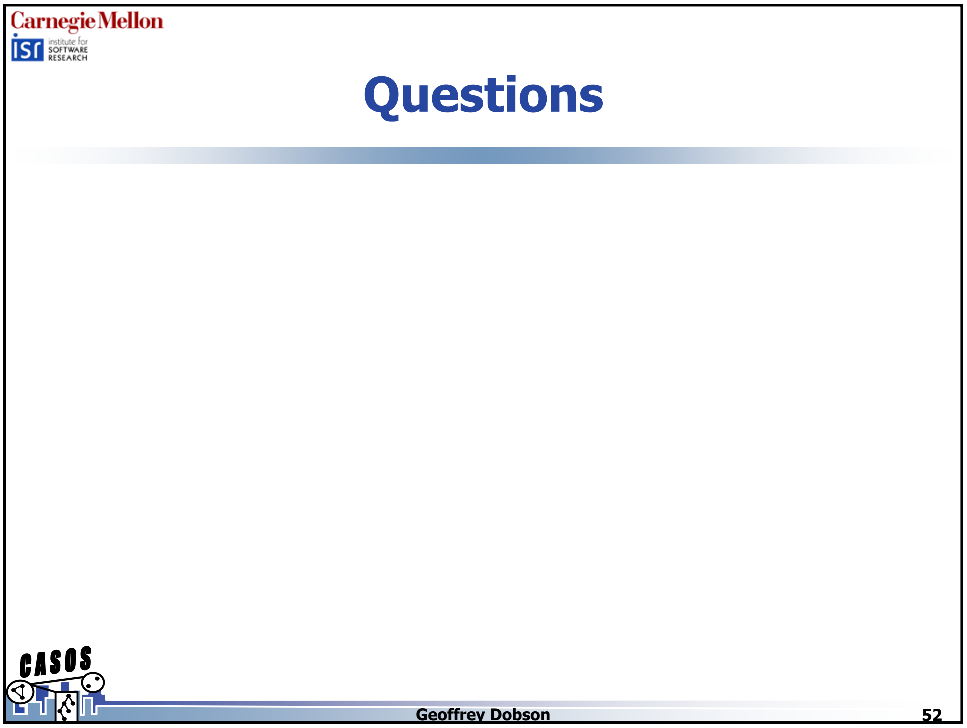
Model Validation Plan

7. Theory Validation

Guiding Question:

Does the model make a valid use of the theory?

Computational methodology
and formulas documented



Questions