UCCS

University of Colorado
Colorado Springs

UCCS CyberRecon Project

TEMPS: A Framework for Quantifying Cyber Operations Success against Adversarial Threats

Students:

Kora Gwartney, Ekzhin Ear, Jose Luis Castanon Remy, Samuel Oglegba, and Graeme Slack

Academic Advisor:

Professor Dr. Shouhuai Xu

USCYBERCOM Mentors:

LTC Steve Gerber (Ret) (J2 Intelligence)

Mr. John Scully (J5/Cyberspace Planning and Policy)

Presentation POC: Ekzhin Ear - eear@uccs.edu

USCYBERCOM CyberRecon Questions

(inspired the present project)

These two CyberRecon questions are incorporated into the following scientific research problem:

Problem Statement: **How can we enable USCYBERCOM staff and key leaders in their planning of defensive cyberspace operations through a quantitative risk-informed approach?**

Rationale: One solution resolves both questions.

Our Solution Concept: TEMPS Framework

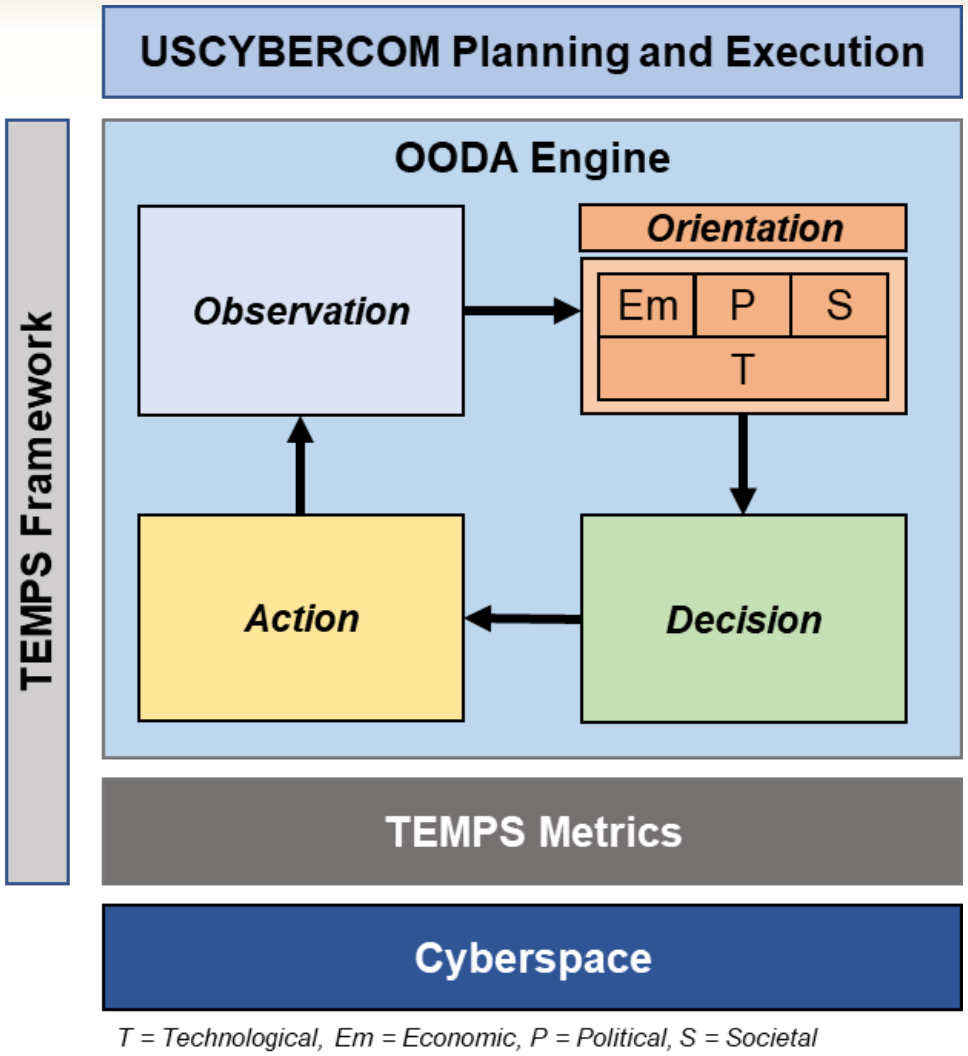


*Illustration colors for emphasis; no additional meanings

TEMPS core: multi-dimensional/ inter-disciplinary impact metrics and analysis:

- T: Technological
- EM: Economic
- P: Political impact
- S: Societal impact

e.g., informs Persistent Engagement and Defend Forward ops

Note: TEMPS extends beyond PMESII-PT

TEMPS objective:

- Quantify TEMPS impacts of USCYBERCOM cyber operations to enhance CDR decision-making through increased *timeliness* and *validity*

TEMPS proof-of-concept via notional case study:

- USCYBERCOM conducts DCO ISO USEUCOM's kinetic operations in Ukraine (next slide)

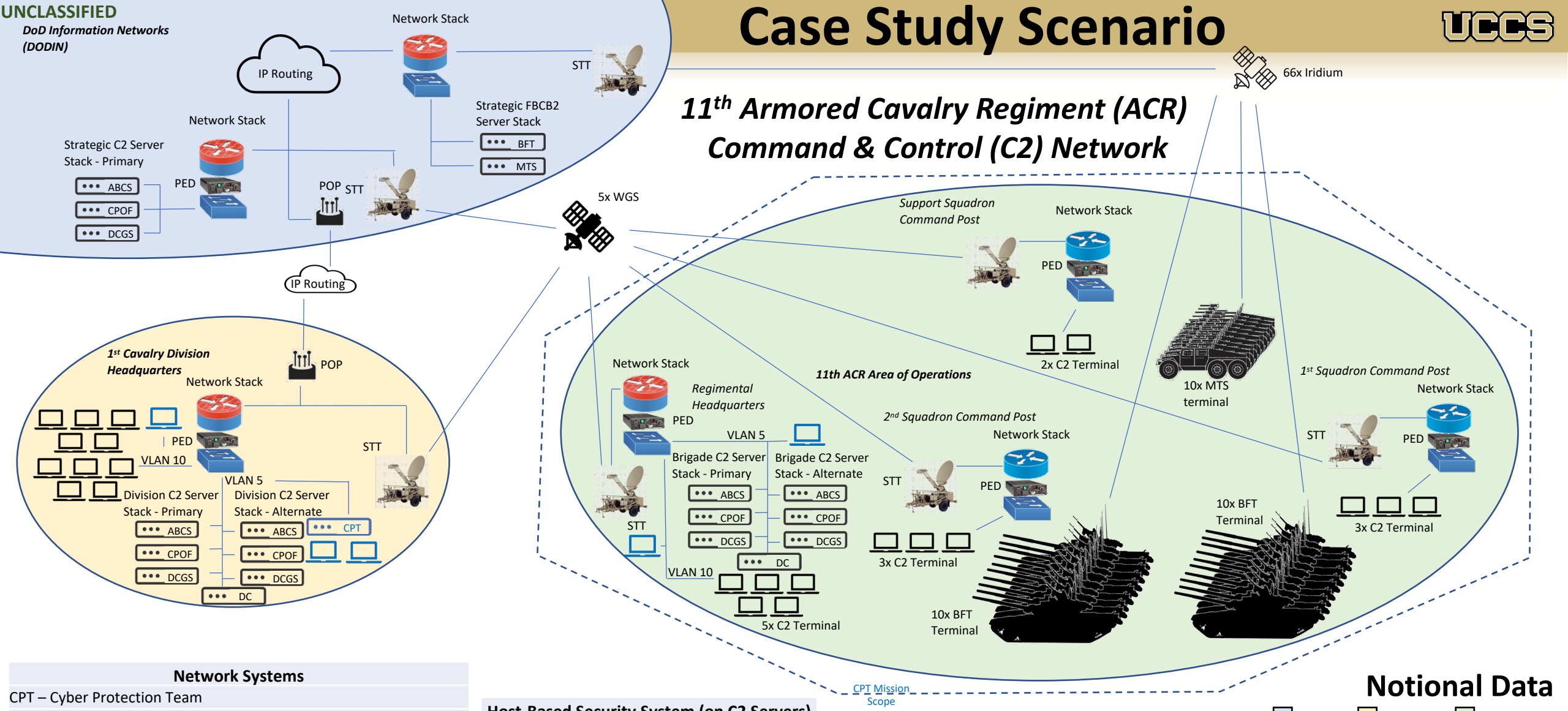
Case Study Scenario

UCCS

UNCLASSIFIED

DoD Information Networks (DODIN)

11th Armored Cavalry Regiment (ACR) Command & Control (C2) Network



Notional Data

DODIN | 1CAV AO | 11ACR AO

Network Systems
CPT – Cyber Protection Team
Iridium – Commercial communications satellite constellation
NIPR – Non-classified Internet Protocol Router Network
PED – Portable Encryption Device
POP – Point of Presence
SIPR – Secure Internet Protocol Router Network
STT – Satellite Transportable Terminal
WGS – Wideband Global Satellite communications constellation

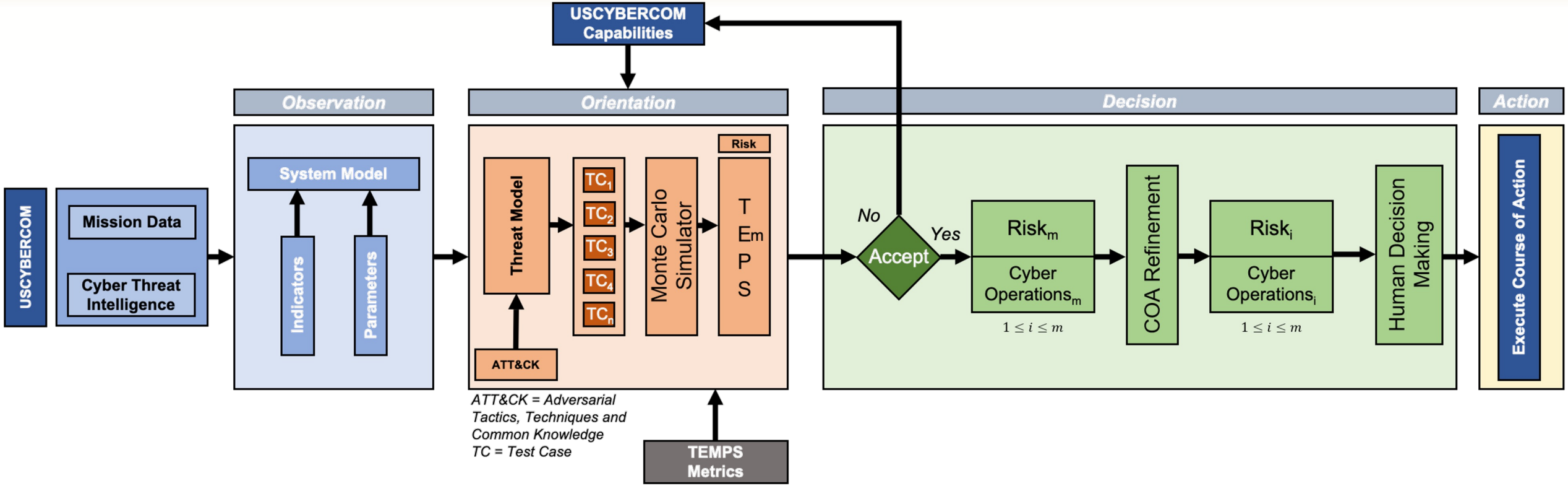
Host-Based Security System (on C2 Servers)
McAfee Antivirus
McAfee Endpoint Protection
McAfee Data Loss Prevention

Endpoint Detection & Response Suite (on Domain Controller(DC))	
Snort	McAfee ePolicy Orchestrator
Nessus	SolarWinds

Information Systems
ABCS – Army Battle Command System
CPOF – Command Post of the Future
DCGS-A – Distributed Common Ground System - Army
FBCB2-BFT – Force XXI Battle Command Brigade-and-Below - Blue Force Tracker
FBCB2 MTS – Movement Tracking System

UNCLASSIFIED

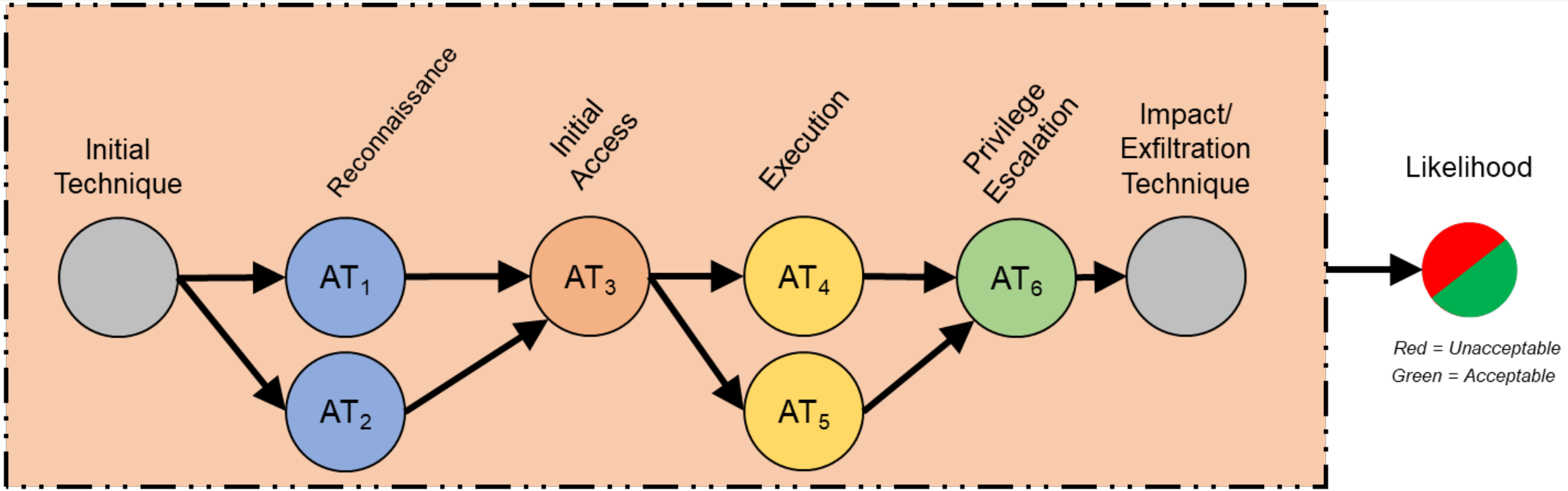
A Specific Instantiation of the TEMPS Framework



Key Idea - Uses TEMPS metrics: ***measures*** technological, economic, political, and societal *risks* per cyber operation via simulation; ***characterizes*** mission risks; ***enhances*** staff's COA Dev, Analysis & Wargaming, and Comparison; ***informs*** CDR's COA Approval decision (see paper for details)

**Illustration colors for emphasis and corresponds to TEMPS framework colors; no additional meanings*

An Example Test Case



AT = Attack Technique

Deep dive into the Orientation (analysis) phase: Simulation using Monte Carlo of ***potential attacker paths*** via red tactics and techniques across areas of influence ***in blue cyber terrain***

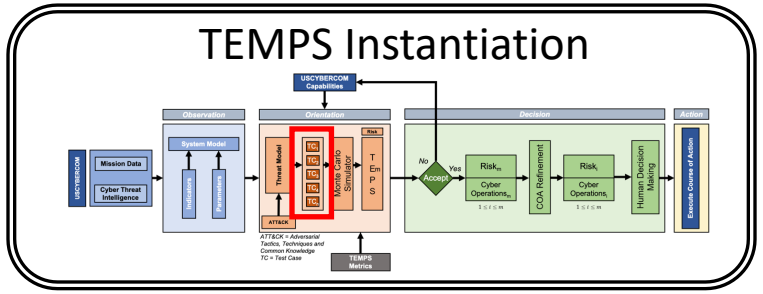


**Illustration colors for emphasis except as noted for Likelihood; no additional meanings*

TEMPS Aims to Answer for USCYBERCOM:

(sample questions)

- How many *zero-day exploits* must the adversary employ to defeat a CPT DCO mission ISO a multi-domain operation?
- How many *exquisite cyber capabilities* (e.g., zero-day exploits, classified malware signatures) must CNMF/JFHQ-C/JFHQ-DODIN employ in a particular cyber operation to attain mission assurance greater than 90% probability?
- What cyber operations and capabilities must USCYBERCOM employ to ensure an *economic consequence* (i.e., negative impact) of a Hunt Forward operation is below the predetermined threshold with a greater than 90% probability?
  - Likewise, for a predetermined *political consequence* threshold
- What would be the *societal consequences* from USCYBERCOM's decision to not conduct a CNMF NMT operation to thwart adversarial influence operations on U.S. citizens?

The TEMPS Framework and the Way Forward

- **Problem:** Enable USCYBERCOM defensive cyberspace operations planning through a quantitative risk-informed approach
- **Progress:**
  - A proof-of-concept TEMPS tool
- **Next Steps:**
  - Systematic and comprehensive metrics development
  - Observation and Orientation process development
  - TEMPS software implementation

(see paper for more information)

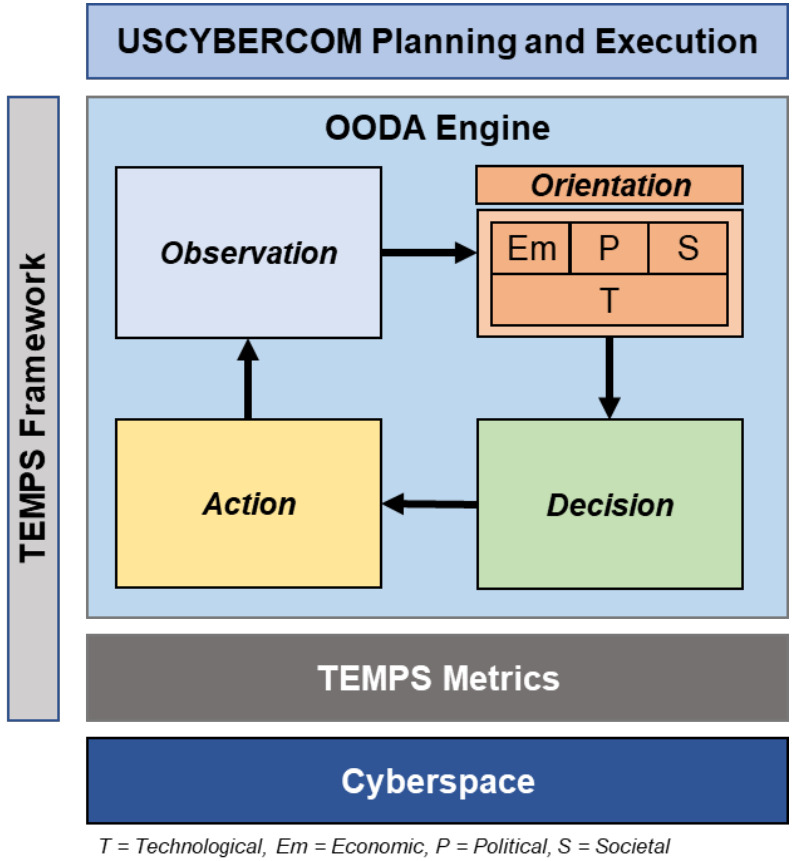


*Illustration colors for emphasis; no additional meanings

Thank you!

Presentation POC: Ekzhin Ear - eear@uccs.edu

University of Colorado
Colorado Springs