Claremont McKenna College
Thesis 2022

CYBER WARGAMES

SARAH CHEN

AGENDA

- Research Methodology
- Why Build Cyber Wargames
- Key Elements:
  - Purpose
  - Scenario
  - Capabilities
- Methodology for Game Analysis
- Games Analyzed
- Findings and Suggestions:
  - Limitations
  - Problems
- Broad Steps for the Future
- Build Cyber Wargames

KEY POINTS

CYBER WARGAMES ARE A USEFUL TOOL TO UNDERSTAND CYBER CONFLICT

THEY PRESENT UNIQUE AND INTERESTING DESIGN CHALLENGES

THE BEST WAY TO OVERCOME THOSE DESIGN CHALLENGES IS TO EXPERIMENT WITH GAME DESIGN

WE SHOULD BUILD MORE CYBER WARGAMES

RESEARCH METHODOLOGY

CYBERSPACE AND WARGAMING ACADEMIC LITERATURE

INTERVIEW WITH EXPERTS

Jennifer McCardle
John Curry
Tom Mouat
Reid Pauly
Catherine Lea
Frank Smith
Erik Lin-Greenberg
Don Marrin
Jason Vogt
Peter Pellegrino
Yuna Wong
Andrew Haggman
Jeremy Sepinsky
Elcin Ada Sayin
Sebastian Bae
Brandon Valeriano
Elizabeth Bartels

GAME ANALYSIS

WHY BUILD CYBER WARGAMES?

Cyberspace, attacks, and strategies are difficult to understand, particularly from a decision-maker perspective

- New and dynamic
- Covert and classified
- Highly technical
- No ’testing’ arena
- No norms or red-lines

WHAT MAKES A GOOD CYBER WARGAME?

Who is it built for?

What do they want?

Does your game do that?

KEY ELEMENTS

Purpose: Analytical

Explore a Cyber Concept

- Explore the Understanding of Existing Cyber Policies
- Explore Communications within a Cyber Context
- Understand How Cyber Operations Affect Kinetic Infrastructure

Develop or Test Cyber Plans or Include Cyberspace into Existing Plans

- Test the Effectiveness of Current or Future Cyber Response Policies
- Assess the Integration of Cyber Warfare in Multi-Domain Conflict
- Identify Potential Failures or Weakpoints

Assess Cyber-Related Decision-Making Through Experiments

- How Decision-Makers Will Respond to Cyber Attacks of Varying Levels
- Assess How Conflict Could Arise through Cyber-Attacks

Speculate on Future Technology Capabilities and Scenarios

- Speculate on the Cyber Goal-Posts
- Extend Capabilities through Technology

Refine Cyber Response Plans

KEY ELEMENTS

Purpose: Educational

Education, Exercise, and Training

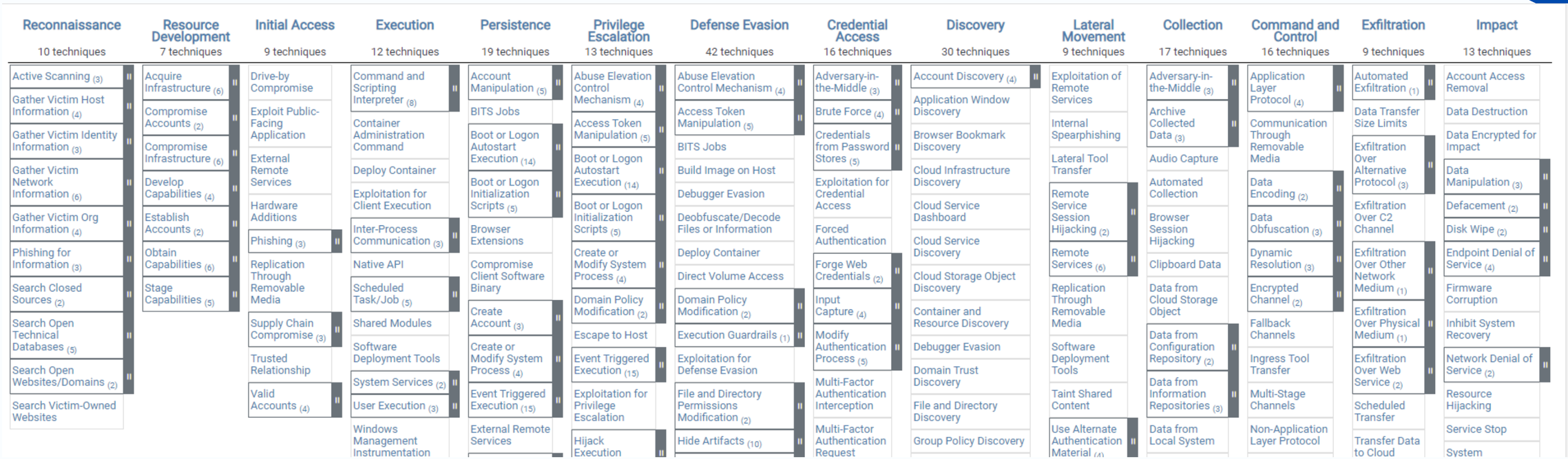
Exercise a Cyber Response Plan

Act as a Communications Tool Between Cyber and Non-Cyber Experts

Teach Non-Experts Cyber Concepts

KEY ELEMENTS

Fidelity and Realism



The Cyber Kill-Chain:

Who launches what against whom, why, and how?

What - Tools/Techniques

How - Delivery/Techniques

Why - Effects

Simulating the 'Fog' of Technology and War

KEY ELEMENTS

Cyber Capabilities

Focus or Support of the Operation?

Fixed or Matrix'd?

- Argumentation Mechanics

Tactical, Operational, or Strategic

Covert or Overt?

Past, Present, or Future?

- Extrapolation, Interpolation, and Imagineering

METHODOLOGY FOR ANALYSIS

- Game
- Purpose
- Specific Objective
- Sponsor
- Format
- Participants and Interaction
- Adjudication
- Cyber Representation
- Data Generated
- Ideal Outcome and Audience

Cyber Representation:

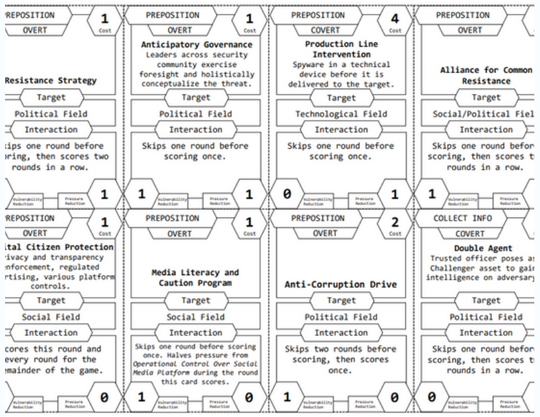
- Cyber Game or Cyber-In-Game
- Fixed or Matrix'd
- Tactical, Operational, or Strategic
- Covert or Overt
- Past, Present, or Future
- Technical Detail Level
- Cyber Kill Chain: Cause or Effect
- Chance Mechanics

Games Analyzed

Analytical

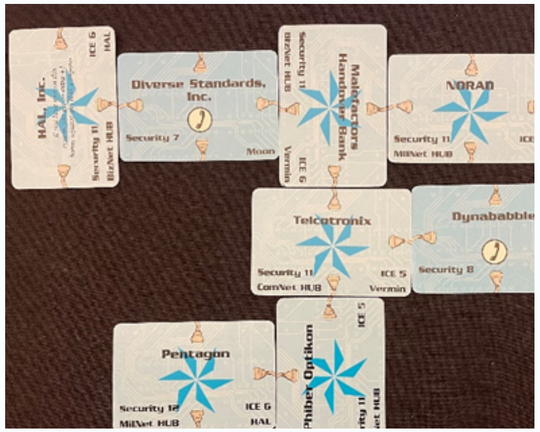
- Cyber Storm Series
- Global Title X Series
- Defend Forward Critical Infrastructure

Educational



- MERLIN Off-the-Shelf
- Hybrid Threat Rising
- Cyber Card Game
- Littoral Commander
- Cyber Security Strategy
- Enterprise Defender
- Collection Deck
- Influence 2040

Entertainment



- CIA Collect It All
- Hacker: Steve Jackson
- [d0x3d!]

FINDINGS: LIMITATIONS

Cyber Representation is a Guessing Game

- CONSTANTLY CHANGING CAPABILITIES
- CLASSIFICATION AND LIMITED INFORMATION
- OVERSIMPLIFICATION OR COMPLICATION WITH FIXED CAPABILITIES

  False Action-Reaction Dynamic
- OVERCOMPLICATION THROUGH TECHNICAL JARGON
- EXPERTS DIFFER - SME VARIABILITY
- NO STANDARDIZATION OF REPORTING DESIGN, ANALYSIS, OR DATA

FINDINGS: PROBLEMS

- PURPOSES THAT ARE TOO LARGE OR ATTEMPT TO VERIFY/PREDICT AN OUTCOME
- STRATEGIC AND OPERATIONAL LEVEL GAME INTEGRATION
- PSYCHOLOGICAL EFFECT REPLICATION OR INFORMATION SUSPICION
- ARBITRARY FINITE OPERATIONS
- DATA CAPTURE
- BUDGET, TIME, AND EXPERTISE
  Top-Heavy Field

Accept that unclassified, and potentially classified, games cannot accurately represent the cyber attack-defense framework

BROAD STEPS FOR THE FUTURE

ACCEPTANCE OF LIMITATIONS

Educational vs. Analytical

TALENT DEVELOPMENT

No games without designers

MORE GAMES, TEST PROBLEMS

Smaller-scale, rapid games

Experimentation

Unclassified Games

RIGOROUS REPORTING AND DATA SHARING

Repository of Mechanics and Reports

BUILD CYBER WARGAMES

Player can experiment with decisions for cyberspace, attacks, and strategies through cyber wargames

- Update with new and dynamic capabilities
- See the effects of covert and classified operations
- Simplify highly technical concepts
- Operate as a 'testing' arena
- React to norms and red-lines

Claremont McKenna College
Thesis 2022

QUESTIONS, COMMENTS, ACCESS TO THESIS:

EMAIL CONTACT

CHEN.Y.SARAH@GMAIL.COM