

# CYBER WARGAMES

SARAH CHEN

Claremont McKenna College

Thesis 2022



# 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

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

# KEY POINTS



# 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?**

## 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



# Fidelity and Realism

# KEY ELEMENTS

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Access Token Manipulation (5)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoded Through Removable Media	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Escape to Host	Domain Policy Modification (2)	Modify Authentication Process (5)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	Execution Guardrails (1)	Multi-Factor Authentication Process (5)	Debugger Evasion	Use Alternate Authentication Material (1)	Data from Information Repositories (3)	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Domain Trust Discovery			Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (2)
			User Execution (3)	External Remote Services	Hijack Execution	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request	File and Directory Discovery			Non-Application Layer Protocol	Transfer Data to Cloud	Resource Hijacking
			Windows Management Instrumentation			Hide Artifacts (10)		Group Policy Discovery					Service Stop
													System

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

## 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

<p>REPOSITION OVERT 1 Cost</p> <p>Resistance Strategy</p> <p>Target</p> <p>Political Field</p> <p>Interaction</p> <p>Skips one round before scoring, then scores two rounds in a row.</p>	<p>PREPOSITION OVERT 1 Cost</p> <p>Anticipatory Governance</p> <p>Leaders across security community exercise foresight and holistically conceptualize the threat.</p> <p>Target</p> <p>Political Field</p> <p>Interaction</p> <p>Skips one round before scoring once.</p>	<p>PREPOSITION COVERT 4 Cost</p> <p>Production Line Intervention</p> <p>Spyware in a technical device before it is delivered to the target.</p> <p>Target</p> <p>Technological Field</p> <p>Interaction</p> <p>Skips one round before scoring once.</p>	<p>PREPOSITION OVERT</p> <p>Alliance for Common Resistance</p> <p>Target</p> <p>Social/Political Field</p> <p>Interaction</p> <p>Skips one round before scoring, then scores two rounds in a row.</p>
<p>REPOSITION OVERT 1 Cost</p> <p>Digital Citizen Protection</p> <p>Privacy and transparency enforcement, regulated routing, various platform controls.</p> <p>Target</p> <p>Social Field</p> <p>Interaction</p> <p>Skips this round and every round for the remainder of the game.</p>	<p>PREPOSITION OVERT 1 Cost</p> <p>Media Literacy and Caution Program</p> <p>Target</p> <p>Social Field</p> <p>Interaction</p> <p>Skips one round before scoring once. Halves pressure from Operational Control Over Social Media Platform during the round this card scores.</p>	<p>PREPOSITION OVERT 2 Cost</p> <p>Anti-Corruption Drive</p> <p>Target</p> <p>Political Field</p> <p>Interaction</p> <p>Skips two rounds before scoring, then scores once.</p>	<p>COLLECT INFO COVERT</p> <p>Double Agent</p> <p>Trusted officer poses as Challenger asset to gain intelligence on adversary.</p> <p>Target</p> <p>Political Field</p> <p>Interaction</p> <p>Skips one round before scoring, then scores two rounds in a row.</p>

- 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



## 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

**BROAD  
STEPS FOR  
THE  
FUTURE**



# 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**



**QUESTIONS, COMMENTS, ACCESS TO THESIS:**

**EMAIL CONTACT**

**CHEN.Y.SARAH@GMAIL.COM**

Claremont McKenna College

Thesis 2022

