INSTITUTE FOR DEFENSE ANALYSES

# Cyber Maneuver, Operations, and Combat: A Knowledge Wargame (CMOCKW)

Dr. Walter R. Dodson, III, Project Leader

2LT Taylor Bradley

October 2022

Approved for Public Release.

Distribution Unlimited.

IDA Document NS D-33213

Log: H 2022-000353

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication
This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-19-D-0001, 2377.02 Joint & Cyber Test & Evaluation, for the Office of the Director, Operational Test and Evaluation. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments
The IDA Technical Review Committee was chaired by Dr. V. Bram Lillard and consisted of Erick D McCroskey from the Operational Evaluation Division, and Joanna C. Di Scipio, and Yuna H. Wong from the JAWD Division.

For more information:
Dr. Walter R. Dodson, III, Project Leader
swhetsto@ida.org Dodson •703-845-2424

Dr. V. Bram Lillard, Director, Operational Evaluation Division
vlillard@ida.org • (703) 845-2230



Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-33213

# Cyber Maneuver, Operations, and Combat: A Knowledge Wargame (CMOCKW)

Dr. Walter R. Dodson, III, Project Leader

2LT Taylor Bradley

# Executive Summary

Historically, the Director, Operational Test and Evaluations' (DOT&E's) congressionally-mandated Cyber Assessment Program (CAP) has proven its unique value to DoD by collecting ground truth tactical data on the back-and-forth of cyber conflict between DoD Cyber Red Teams that emulate our adversaries and the DoD cyber defenders. These assessments, typically taking place during Combatant Command or Service Tier 1 exercises, also characterize the strategic interactions between senior DoD officials. However, operational-level decision-making is less thoroughly examined because of the necessity of ensuring commanders' training objectives are met, and because of legal or risk factors that prohibit destructive activity by DoD Cyber Red Teams on commercial, civilian, and social media networks and applications.

DOT&E directed IDA to develop a cyber wargame that will enable DoD organizations to explore operational-level decisions regarding cyberspace force employment and network security postures. The IDA-designed wargame, *Cyber Maneuver, Operations, and Combat: A Knowledge Wargame (CMOCKW)*, realistically emulates the nature of operational cyber conflict with a dynamic Opposing Force (OPFOR) that has a chance to "win," a double-blind approach that replicates cyber uncertainties by revealing limited information to each side, and a force-on-force approach that uses capability values assigned to friendly and enemy units and networks to facilitate semi-hidden, stochastic adjudication, and a "gloves off" approach that does not unrealistically constrain the OPFOR.

CMOCKW may be planned and executed at the SECRET or higher classification level as desired, simulates one week of "real scenario time" in a one-hour game turn, can be tailored and scaled to examine the decisions and cyberspace terrain desired by the "customer," and is relatively simple and "lightweight" to plan, teach, and execute.

IDA began development of CMOCKW in April 2021 and has executed four playtests with participants drawn from the CAP and other DoD partners. With DOT&E's enthusiastic support, IDA presented this overview of CMOCKW at the Connections US 2022 Wargaming Conference on July 27, 2022.

# Cyber Maneuver, Operations, and Combat: A Knowledge Wargame

# (CMOCKW)

2LT Taylor Bradley

Connections Wargaming Conference

JULY 2022

**Institute for Defense Analyses**

4850 Mark Center Drive ● Alexandria, Virginia 22311-1882

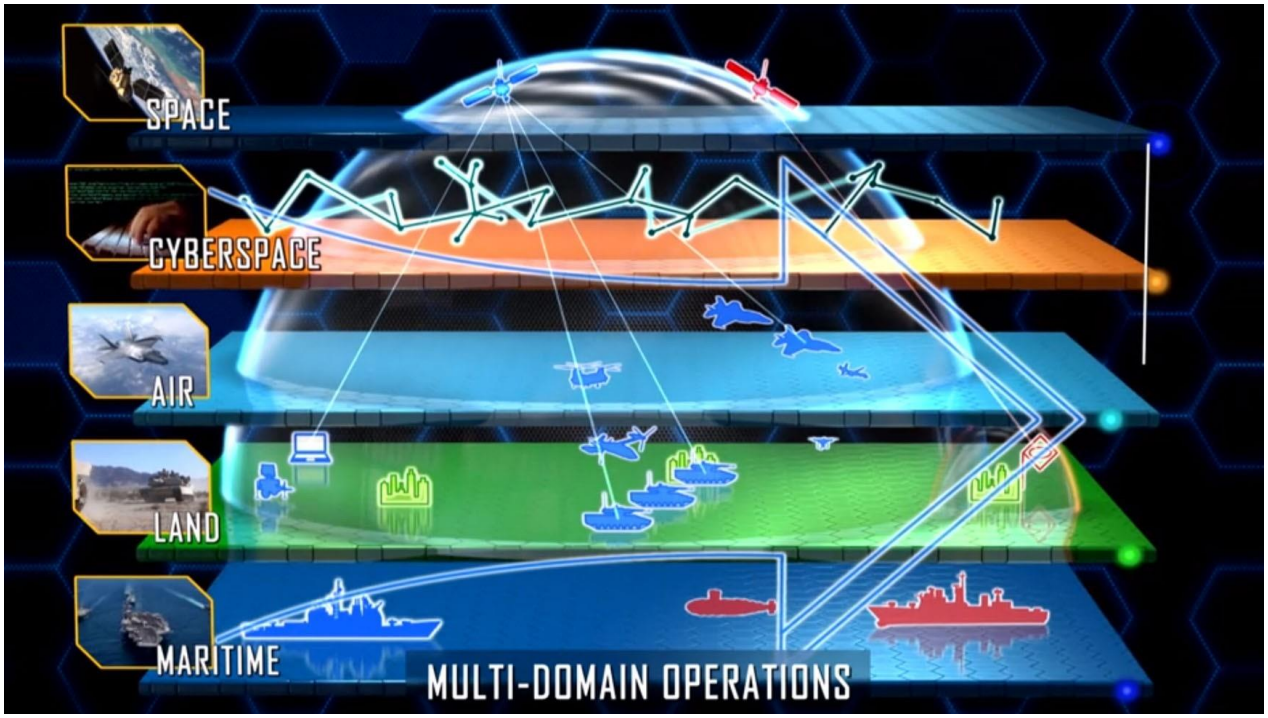
Attachment

# Agenda

1. Cyber wargaming background
2. CMOCKW scope & goals
3. Representation of cyberspace
4. Key takeaways
5. Future work

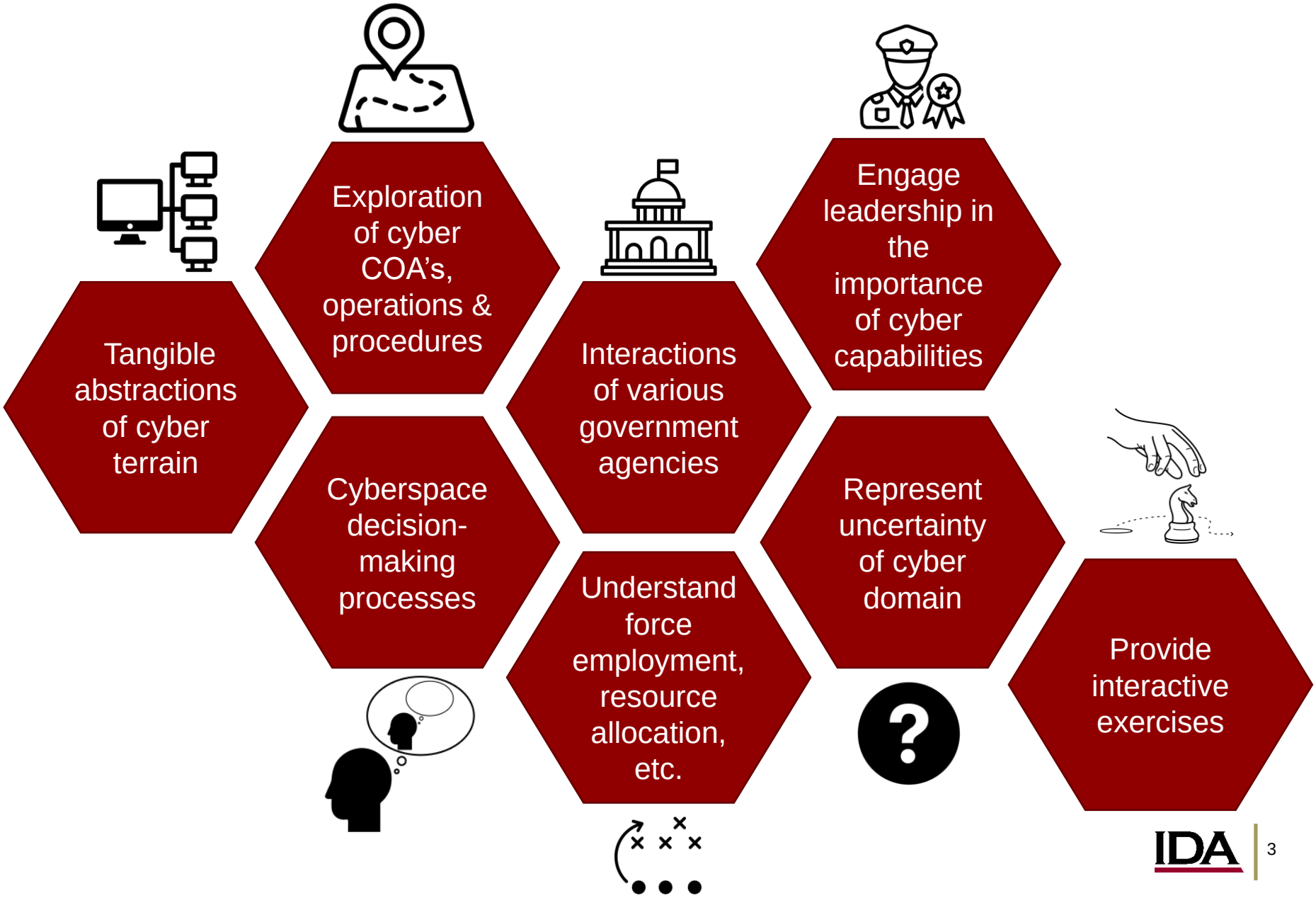
# The cyber domain is underexplored and misunderstood

- Multi-Domain Operations
  - Increasing relevance of cyberspace
  - Complex new operational environment
- Adopting and creating doctrine
  - Lack of operational level cyber doctrine
  - Grounding in accepted practice & industry standard
  - MITRE ATT&CK, NIST 800-53, etc.




Acronyms: ATT&CK - Adversarial Tactics, Techniques & Common Knowledge; NIST - National Institute of Standards and Technology

# Cyber wargaming provides many benefits.



# CMOCKW[1] is a one-of-a-kind operational-level cyber wargame!

- Explore cyberspace decision-making
- Represent uncertainty
- Model attack & defense
- Virtual terrain
- Incorporate risk management, intel decisions, force employment, etc.


- [1]Name chosen as a memorial to Mr. Chuck Mock (IDA/OED)

# We plan to make CMOCKW versatile and applicable to many government organizations & industries.

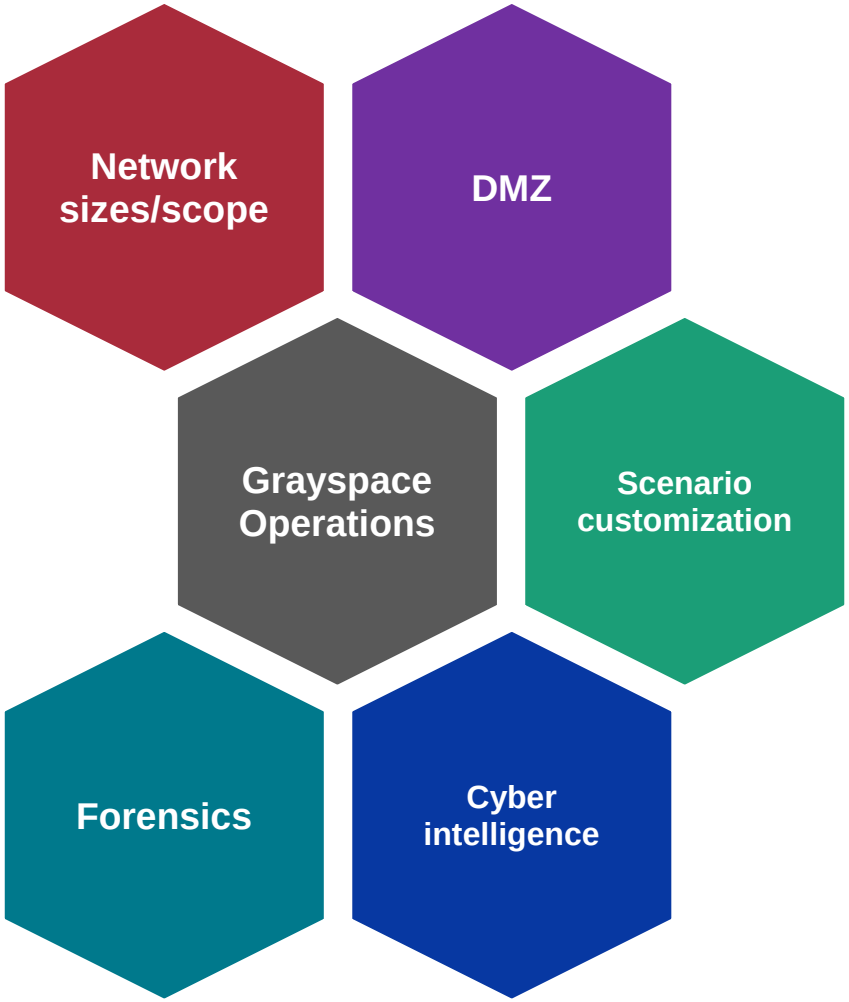
## Short term

- Use by DoD Sponsor
  - Available for cyber assessments
  - Plan to execute 2 wargames in FY23
- Use by various DoD organizations

## Long term

- Publicly available
- Commercial purchase options
  - Non-profit basis for IDA

# CMOCKW is customizable for various needs/scenarios



# Here's how a turn of CMOCKW is played:

1 turn = 1 week

**Phase 1:** Strategic Update

**Phase 2:** Intel COA Analysis

**Phase 3:** DCO Operations

**Phase 4:** Intel Targeting

**Phase 5:** OCO Operations

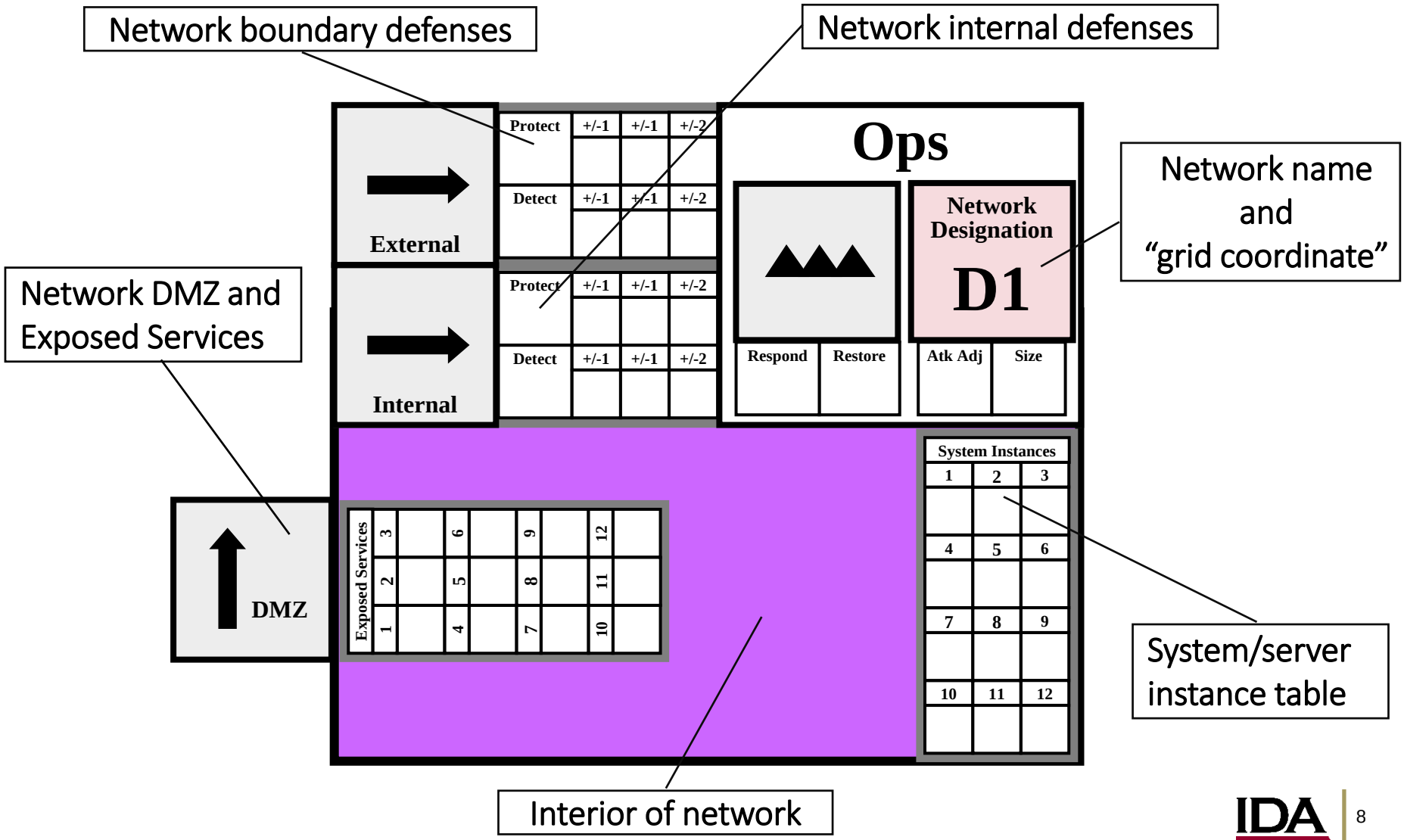
**Phase 6:** Strategic Requests

**Phase 7:** Intel Collection Management

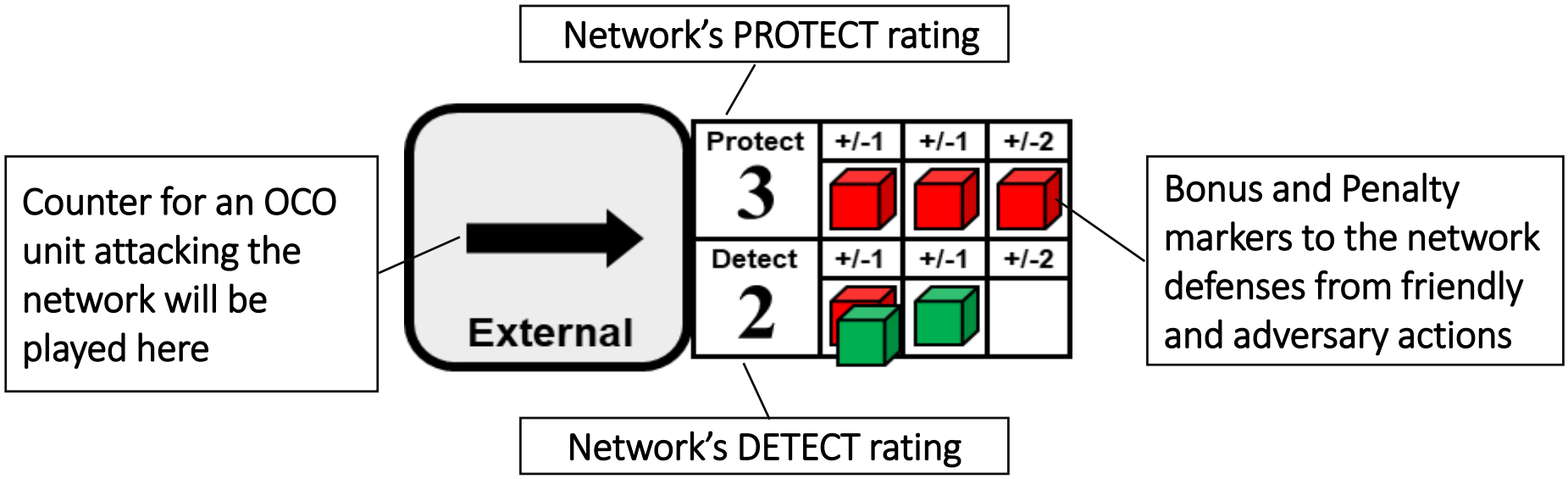
**Phase 8:** End of Turn

Acronyms: COA – Course of Action; DCO – Defensive Cyber Operations; OCO – Offensive Cyber Operations

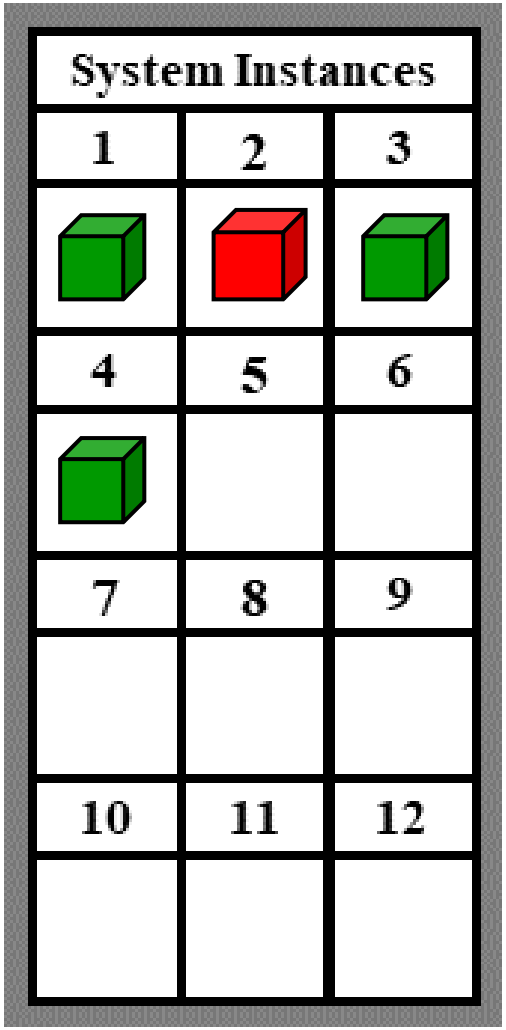
# Tangible representation of cyberspace using abstraction



# Tangible representation of cyberspace using abstraction

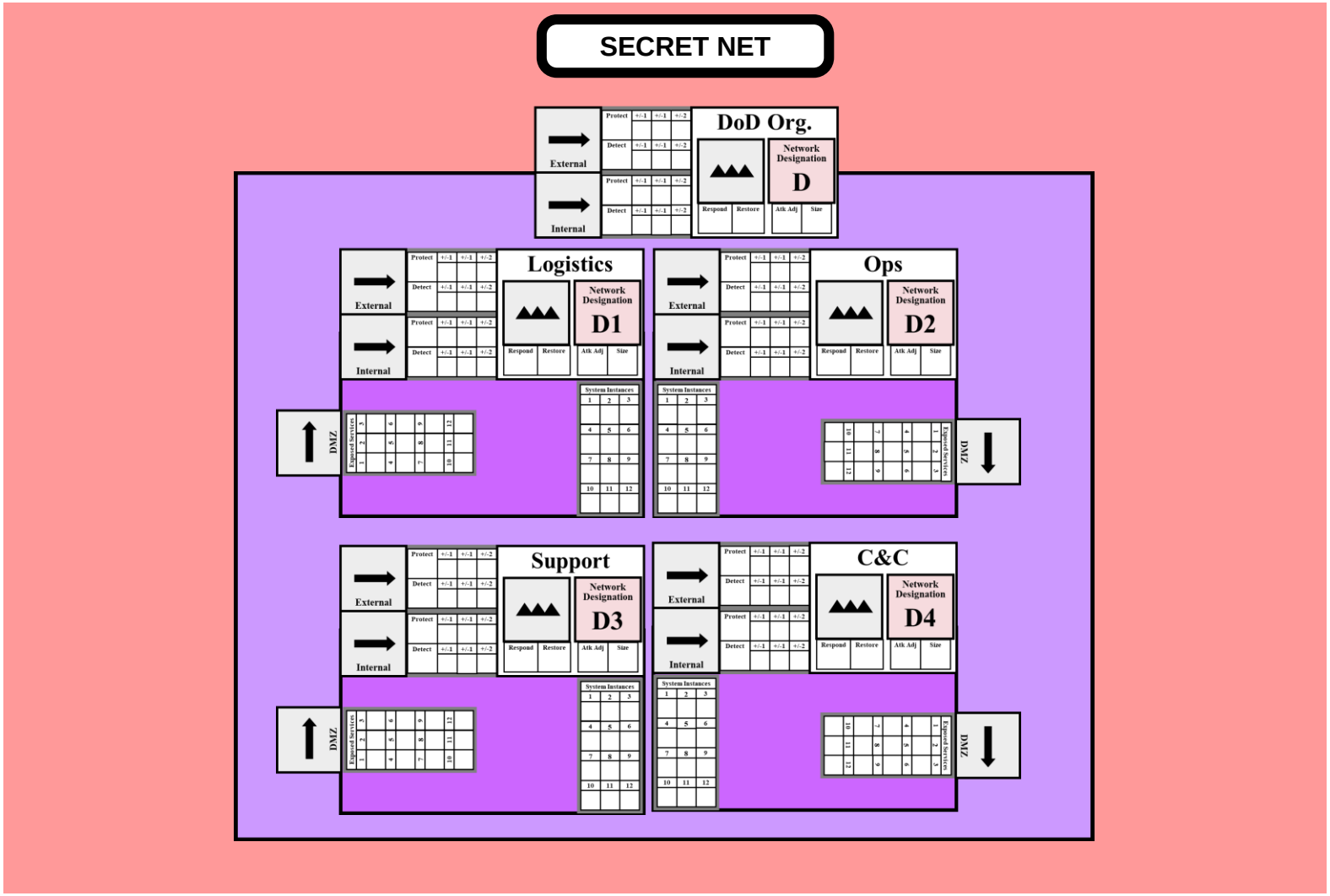


# Tangible representation of cyberspace using abstraction

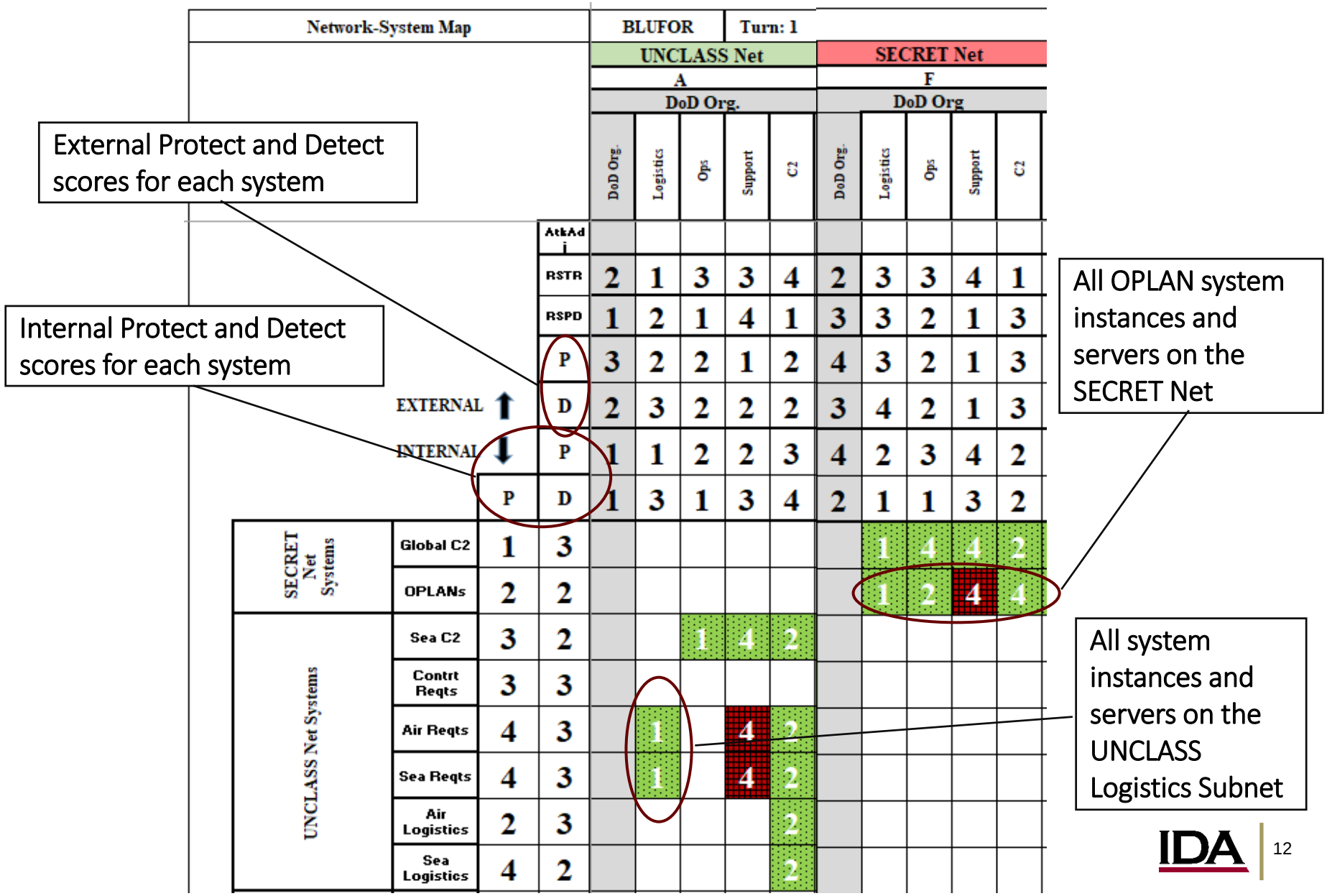



| System Instance | System name |
|---|---|
| 1 | Data Management |
| 2 | OPLANS |
| 3 | Personnel Data |
| 4 | Targeting |

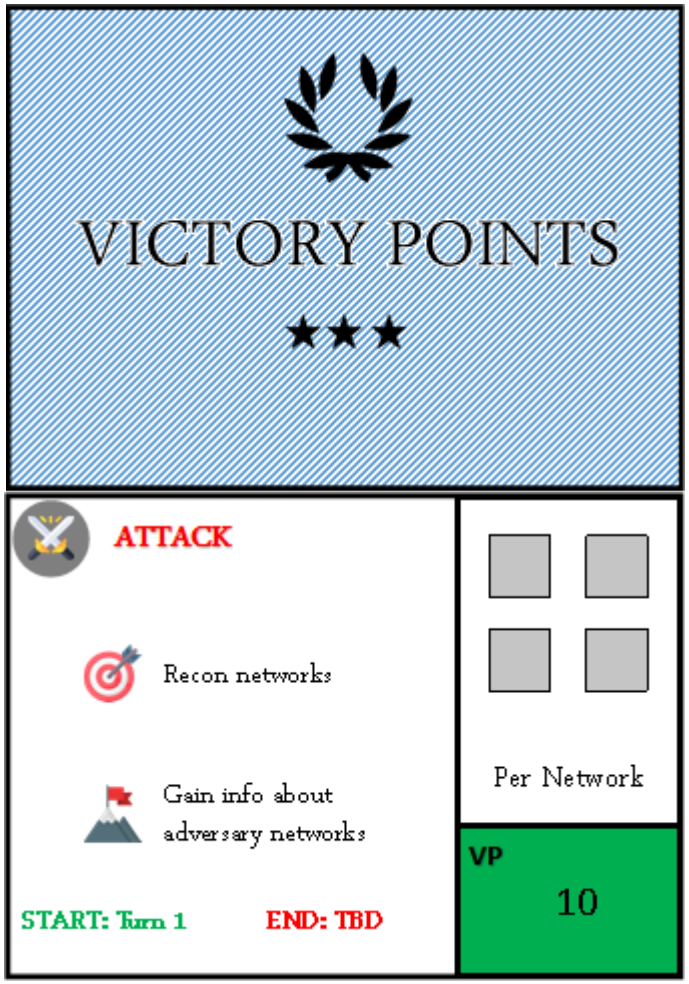
# Tangible representation of cyberspace using abstraction

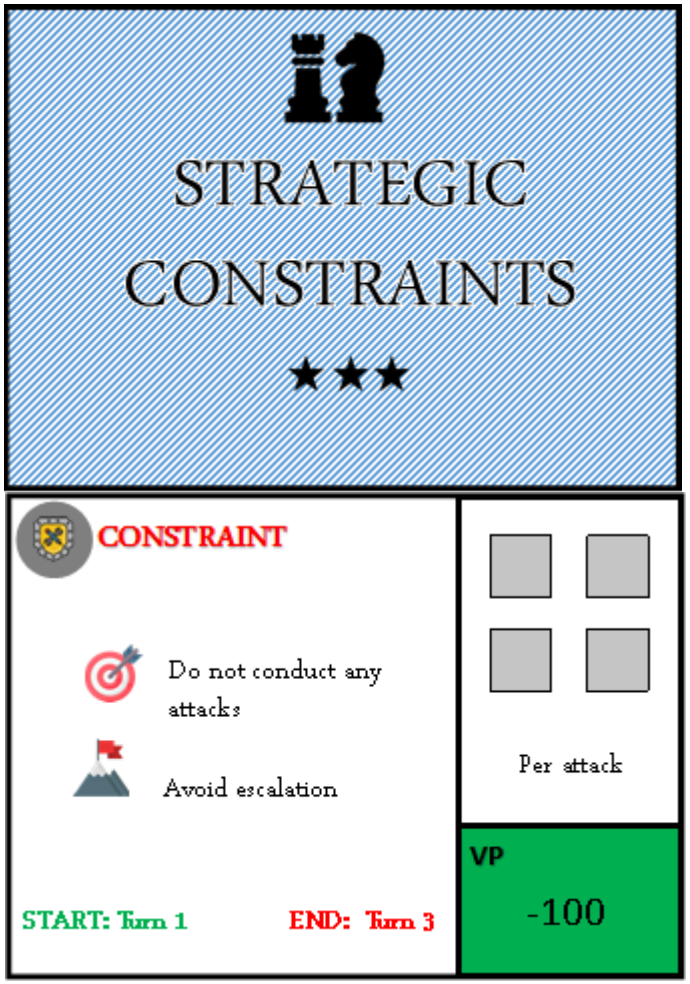


# Network-System Map

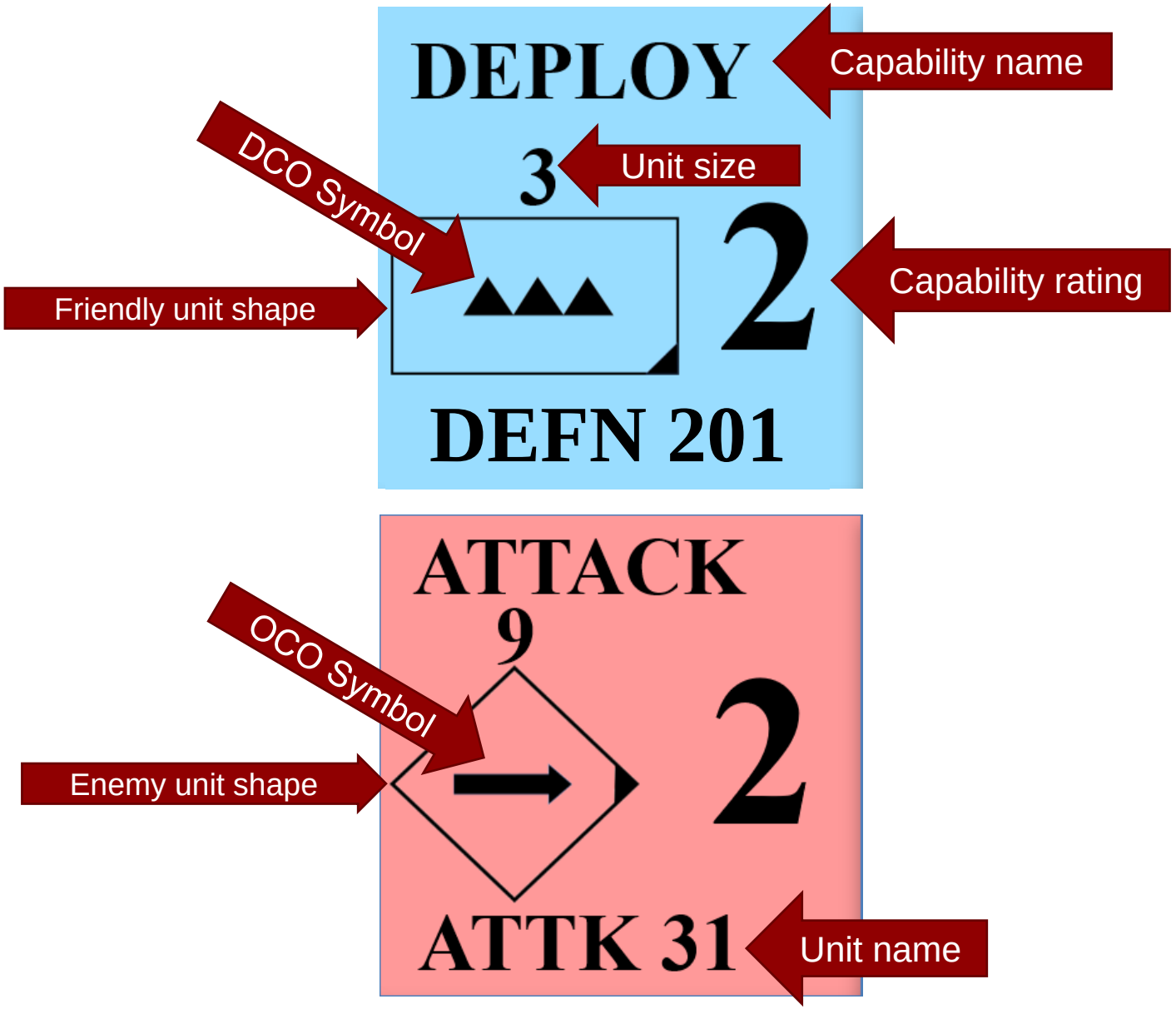


# Players are provided with goals, objectives, and constraints to drive gameplay



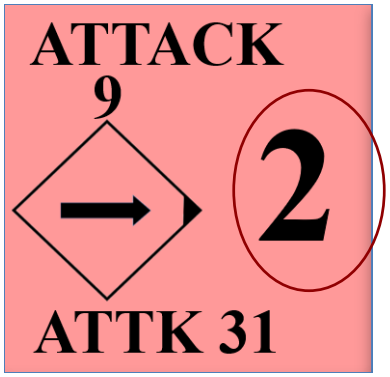



# Cyber unit counters created using doctrine and symbology



# Combat adjudication when a cyber-on-cyber attack occurs

| ACTION ADJUDCIATION | Capability Differential | | | | | | |
|---|---|---|---|---|---|---|---|
| d20 Die Roll | -3 | -2 | -1 | 0 | +1 | +2 | +3 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 |
| 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 |
| 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 |
| 13 | 13 | 13 | 13 | 13 | 13 | 13 | 13 |
| 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 |
| 15 | 15 | 15 | 15 | 15 | 15 | 15 | 15 |
| 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |
| 17 | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 |
| 19 | 19 | 19 | 19 | 19 | 19 | 19 | 19 |
| 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 |




vs.


+


=

Success or failure
AND
Detection or evasion

# Here is where CMOCKW is headed

Playtest 5:

August 8-12, 2022

Wargame executed in the field for DoD organizations

Publish a commercially available version

# There are many lessons to be learned and challenges in the future of cyber wargaming

## Lessons Learned

- Cyber warfighting
  - Interactions with other warfighting components
  - Doctrine & symbology
- Wargaming
  - Uses, benefits, etc.
  - Mechanics
  - Player experience
- DoD interaction with outside agencies

## Challenges

- Tangible depiction of cyber domain & capabilities
- Simplification of cyberspace while keeping it realistic

# Conclusion

## Key Takeaways

- DoD needs wargaming to support cyber decision-making
- CMOCKW is well-positioned to fill this niche

## Potential Payoff

- Expanding cyber doctrine through gameplay
- Getting leadership involved & invested

## Future Game Evolution

- Automated adjudication to speed up gameplay
- Potential integration with existing physical-domain wargames
- Create online version to support remote, multi-location execution

# Questions?

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 01-10-2022 | Final | N/A |

**4. TITLE AND SUBTITLE**

D-33213 Cyber Maneuver, Operations, and Combat: A Knowledge Wargame (CMOCKW)

**5a. CONTRACT NUMBER**

HQ0034-19-D-0001

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

2LT Taylor Bradley

**5d. PROJECT NUMBER**

BD-9

**5e. TASK NUMBER**

2377

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Institute for Defense Analyses
730 East Glebe Road
Alexandria, Virginia 22305

**8. PERFORMING ORGANIZATION REPORT NUMBER**

D-333213

H 2022-000353

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

Director, Operational Test and Evaluation
1700 Defense Pentagon
Washington, DC 20301

**10. SPONSOR/MONITOR'S ACRONYM(S)**

DOT&E

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

Approved for Public Release. Distribution Unlimited.

**13. SUPPLEMENTARY NOTES**

Project Leader: Dr. Walter R. Dodson, III

**14. ABSTRACT**

This presentation provides an overview of an IDA-developed cyber wargame that explores decisions about cyberspace force employment and network security postures. The wargame realistically emulates the nature of operational cyber conflict with a dynamic Opposing Force (OPFOR) that has a chance to “win,” a double-blind approach that replicates cyber uncertainties by revealing limited information to each side, and a force-on-force approach that assigns capability values to friendly and enemy units and networks to facilitate adjudication, and with no unrealistic constraints on the OPFOR. It may be planned and executed at the SECRET level or higher, simulates one week of “real scenario time” per one-hour game turn, can be tailored and scaled to examine the “customer's” decisions and cyberspace terrain, and is relatively simple and “lightweight” to plan, teach, and execute.

**15. SUBJECT TERMS**

Cyber Warfare; Cyberspace Operations; Operational Graphics

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Dr. Walter R. Dodson, III |
| Unclassified | Unclassified | Unclassified | Unlimited | 25 | 19b. TELEPHONE NUMBER *(Include area code)* 703-845-2424 |