The role of cyber competitions in cyber defense education: A case study of National Cyber League (NCL) participation

Ping Wang, Ph.D., CISSP
University Professor, CIS/Cybersecurity
Robert Morris University

Hubert D'Cruze
University of Maryland

Research Overview

- **Focus**
  Cybersecurity competitions in cyber defense education
- **Significance**
  - Large and increasing demand for qualified cybersecurity workforce
  - Demand for technical and non-technical KSAs
  - NCAE-CD designation requirements for cyber competition activities
- **Goal**
  Explore the value of cyber competitions in cybersecurity education through NCL case study

Background

- Observational studies on benefits of cyber competitions
  - Practical learning experience
  - Fun and motivating
  - Integrate hands-on and theory-based learning
  - Professional networking opportunities

- Active learning theory for competitions
  - Individual and social constructivism
  - Interactive and hands-on learning
  - Collaborative learning in team projects
  - Promote higher levels of cognitive learning and critical thinking

Background: Challenge-Based Framework (CBL) Features & Metrics (Nichols, Cator, & Torres, 2016)

1. A **flexible and customizable** framework as a guiding pedagogy for implementation.
2. A **scalable** model with multiple points of entry.
3. A **free and open system** free from proprietary ideas, products, or subscriptions.
4. A **learner-centered** process that emphasizes learners' direction and responsibilities in learning.
5. An authentic environment that **integrates academic standards** with content.
6. A focus on **global ideas and challenges** with localized solutions that are appropriated for all age groups.
7. A real connection between **academic disciplines and real-world experience**.
8. A framework to **develop 21st century (future) skills**.
9. Purposeful use of technology **for research, analysis, organization, collaboration, networking, communication, publication, and reflection**.
10. The opportunity to **empower learners** to make a difference.
11. A method to **document and assess** the learning process and products.
12. An environment for **in-depth reflection** on teaching and learning.

3-phase Model: Engage (explore ideas/challenges), Investigate (ID solutions), and Act (implement)

Case Study: NCL (National Cyber League)

- Biannual, seasonal, all-virtual competition founded in 2011
- Participants: +13,000 students, +650 colleges/HS, 50 states
- Activities: open gym, practice game, individual game, team game
- NCL CTF games reflect 3-phase CBL model:
  1) Explore security concepts and challenges
  2) Identify digital flags/answers
  3) Submit findings/answers for points (individual/team)
- Mission: Prep next generation cybersecurity workforce and apply school learning to real-world challenges
- Fit most of the features and metrics of CBL model

NCL Domains Mapped to CAE-CD KUs

NCL Skills Domains/Categories	CAE-CD Knowledge Units
Open Source Intelligence	Cyber Threats (CTH)
Cryptography	Basic Cryptography (BCY), Advanced Cryptography (ACR)
Log Analysis	Basic Scripting and Programming (BSP), Fraud Prevention and Management
Network Traffic Analysis	Basic Networking (BNW), Network Defense (NDF), Advanced Network Technology and Protocols (ANT), Intrusion Detection/Prevention Systems (IDS), Network Forensics (NWF), Network Technology and Protocols (NTP)
Forensics	Device Forensics (DVF), Digital Forensics (DFS), Host Forensics (HOF), Media Forensics (MEF)
Web Application Exploitation	Databases (DAT), Database Management Systems (DMS), Web Application Security (WAS)
Scanning & Reconnaissance	Cloud Computing (CCO), IA Architectures (IAA), Operating Systems Hardening (OSH), Vulnerability Analysis (VLA)
Enumeration & Exploitation	Operating System Concepts (OSC), Algorithms (ALG), Advanced Algorithms (AAL), Data Structures (DST), Industrial Control Systems (ICS), Linux System Administration (LSA), Operating Systems Administration (OSA), Windows System Administration (WSA), Low Level Programming (LLP), Secure Programming Practices (SPP), Software Reverse Engineering (SRE), Software Security Analysis (SSA), Penetration Testing (PTT)

NCL Domains/Outcomes Mapped to RMU Coursework

Courses	NCL Domains	Sample Shared Learning Outcomes
Networks & Data Communication	Network Traffic Analysis	Identify components of the OSI model; Trace network packet captures and data flow; Use tools for scanning and packet analysis; Identify network typography and design; Identify network security vulnerabilities; Analyze network layers and protocols; Interpret network traffic to determine security practices.
Computer Network Security	Network Traffic Analysis; Cryptography; Open Source Intelligence	Examine network traffic to identify attacks and threats; Scan for vulnerabilities using common tools; Identify cryptographic schemes and use cases; Describe strengths/weaknesses of encryption solutions; Identify general software vulnerabilities and CVEs; Identify properties of SSL, VPN, hashing, PKI.
Ethical Hacking & Advanced Topics in Cyber Defense	Log Analysis; Network Traffic Analysis; Web Application & Exploitation; Scanning & Reconnaissance; Enumeration & Exploitation	Use scripting languages to analyze log files; Identify the elements of a fraudulent transactions; Analyze network traffic to identify intrusion attempts; Identify web security flaws and exploitations; Identify ICS protocols and applications; Scan operating systems for security vulnerabilities; Identify threats and attacks against cloud services; Examine software source code to identify security issues; Demonstrate basic proficiency of command line capabilities Manager users, passwords, and security policies; Audit security logs; Perform penetration testing to identify application security flaws & vulnerabilities.

RMU Student Participation in NCL & Course Performance

NCL Season	NCL Participants (N)	NCL Domains Completion (AVG)	Participant Course Success Rate (AVG)	Overall Course Success Rate (AVG)
Spring 2022	6	79.9%	93.7%	88.4%
Fall 2021	8	75.8%	90.5%	86.1%
Spring 2021	4	81.3%	96.8%	91.2%
Fall 2020	7	73.5%	89.4%	85.3%
Spring 2020	6	61.8%	87.6%	86.8%
Fall 2019	6	65.4%	88.7%	84.6%
Spring 2019	4	57.6%	83.1%	85.7%
Fall 2018	1	66.5%	100%	87.1%

Findings & Conclusions

- ❑ Longitudinal increase in average NCL domain completion rate
- ❑ Higher NCL completion rate occurs with higher course success rate
- ❑ Qualitative Reflections & Comments from Participants
  Fun, enjoyable, challenging, new learning, would do it again
- ❑ Limitations
  Limited data and observations
- ❑ Future research
  1) NCL impact on critical thinking, problem solving, career dev
  2) Comparative study of NCL and other cyber competitions
- ❑ Questions/Suggestions?
- ❑ Thank you!