

# Resources & Further Reading

## Annotated Bibliography for Human-AI Partnership in Cybersecurity Education

### Table of contents

Human-AI Collaboration & Posthuman Pedagogy . . . . .	1
Cybersecurity Education Research . . . . .	3
NICE Framework & Workforce Standards . . . . .	3
How to Use These Resources . . . . .	5

This collection supports educators implementing human-AI partnership approaches in cybersecurity education. Each entry includes practical context for K-12 classroom application.

#### Quick Start: Essential Reading

New to this approach? Start with these three:

1. **Adams & Thompson (2016)** — Practical heuristics for posthuman inquiry in education
2. **Newhouse et al. (2017)** — The NICE Framework foundation document
3. **CYBER.org Standards** — K-12 cybersecurity learning progressions

### Human-AI Collaboration & Posthuman Pedagogy

These works provide theoretical and practical foundations for understanding humans and AI as collaborative partners rather than tool-user relationships.

#### Researching a Posthuman World: Interviews with Digital Objects

**Adams, C., & Thompson, T. L.** (2016). *Researching a Posthuman World: Interviews with Digital Objects*. Palgrave Pivot.

Empirical

**Why This Matters:** Introduces eight practical heuristics for investigating human-technology relationships in educational settings. The “interviewing objects” approach directly informs how we frame AI as a team member with its own capabilities and limitations—exactly the perspective these activities develop in students.

[Publisher Link](#)

## The Posthuman

**Braidotti, R.** (2013). *The Posthuman*. Polity Press.

Theoretical

**Why This Matters:** Foundational text redefining what it means to be human in an age of technological entanglement. Braidotti’s framework helps educators move beyond anthropocentric assumptions—essential for teaching students that effective cybersecurity emerges from human-AI assemblages, not human dominance over tools.

[Publisher Link](#)

## Artificial Intelligence in Education: Promises and Implications for Teaching and Learning

**Holmes, W., Bialik, M., & Fadel, C.** (2019). *Artificial Intelligence in Education: Promises and Implications for Teaching and Learning*. Center for Curriculum Redesign.

Framework

**Why This Matters:** Comprehensive examination of AI’s role in education with practical implications for classroom implementation. Addresses both opportunities and challenges educators face when integrating AI, including equity considerations relevant to the low-resource implementation options in these activities.

[Publisher Link](#)

## Designing Educational Technologies in the Age of AI

**Luckin, R., & Cukurova, M.** (2019). Designing educational technologies in the age of AI: A learning sciences-driven approach. *British Journal of Educational Technology*, 50(6), 2824-2838.

Empirical

**Why This Matters:** Establishes design principles for educational AI that positions technology as a collaborative partner. Their framework for “intelligence augmentation” aligns directly with the partnership model in these activities, where AI contributes pattern recognition while humans provide contextual judgment.

DOI: [10.1111/bjet.12861](https://doi.org/10.1111/bjet.12861)

## Posthumanism and Educational Research

**Snaza, N., & Weaver, J. A.** (Eds.). (2014). *Posthumanism and Educational Research*. Routledge.

Theoretical

**Why This Matters:** Collection exploring how posthumanist theory transforms educational practice. Multiple chapters address technology-mediated learning and challenge traditional human-centered pedagogies—providing theoretical grounding for why “AI as teammate” represents a more accurate and productive framing than “AI as tool.”

[Publisher Link](#)

## Cybersecurity Education Research

Research and frameworks specifically addressing cybersecurity education, including K-12 approaches, hands-on learning, and workforce development.

### K-12 Cybersecurity Learning Standards

**CYBER.org.** (2021). *K-12 Cybersecurity Learning Standards* (Version 1.0).

Official

**Why This Matters:** The definitive K-12 standards document that these activities align with. Provides grade-band progressions and learning objectives that educators can use to connect activities to curriculum requirements. Essential reference for understanding scope and sequence in cybersecurity education.

[CYBER.org Standards](#)

### Cybersecurity Education in K-12: An Exploratory Study

**Catota, F. E., Morgan, M. G., & Sicker, D. C.** (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, 5(1), tyz001.

Empirical

**Why This Matters:** Though focused on Ecuador, this study provides transferable insights into adapting cybersecurity education for resource-constrained environments—relevant for educators implementing these activities in schools with limited technology access.

[DOI: 10.1093/cybsec/tyz001](#)

### Integrating Social Engineering into Cybersecurity Curricula

**Mitnick, K. D., & Simon, W. L.** (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley.

Framework

**Why This Matters:** Classic text on the human factors in cybersecurity that AI systems cannot fully address. Understanding social engineering—where human judgment is essential—helps explain why AI remains a partner rather than replacement in security operations, a key concept in Activity 2 (Ethics in Automated Security).

[Publisher Link](#)

### NICE Framework & Workforce Standards

Official standards and research connecting cybersecurity education to workforce development and career pathways.

#### NICE Framework (NIST SP 800-181)

**Newhouse, W., Keith, S., Scribner, B., & Witte, G.** (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (NIST Special Publication 800-181). National Institute of Standards and Technology.

Official

**Why This Matters:** The foundational workforce framework that these activities explicitly align with. Defines Work Roles, Knowledge areas, Skills, and Abilities that map directly to activity learning objectives. Essential for CTE programs and anyone connecting K-12 activities to career pathways.

[NIST SP 800-181](#)

### NICE Framework Work Role Categories

**NICE.** (2025). *NICE Framework Work Roles* (Version 2.0.0). National Institute of Standards and Technology.

Official

**Why This Matters:** The 2025 update reorganizes work roles and better reflects current workforce needs, including emerging human-AI collaboration requirements. Activities reference specific Work Roles (PR-CDA-001, PR-CIR-001, OV-SPP-002) from this updated framework.

[NICE Framework](#)

### Cybersecurity Workforce Development: A Capability Maturity Model

**Hoffman, L. J., Burley, D. L., & Toregas, C.** (2012). Holistically building the cybersecurity workforce. *IEEE Security & Privacy*, 10(2), 33-39.

Framework

**Why This Matters:** Addresses the systemic challenges in developing cybersecurity talent pipelines. Their maturity model helps educators understand how K-12 activities contribute to long-term workforce development—useful for grant writing and program justification.

[DOI: 10.1109/MSP.2011.181](#)

### From K-12 to Career: Building Cybersecurity Talent Pipelines

**Tobey, D., Pusey, P., & Burley, D.** (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the National Cyber League. *ACM Inroads*, 5(1), 53-56.

Empirical

**Why This Matters:** Demonstrates effective approaches for engaging students in cybersecurity career pathways through competition and collaboration. The team-based, scenario-driven approaches they validate align with the design of these activities.

[DOI: 10.1145/2568195.2568213](#)

### The Cybersecurity Talent Gap

**(ISC)<sup>2</sup>.** (2023). *Cybersecurity Workforce Study*. International Information System Security Certification Consortium.

Official

**Why This Matters:** Annual industry report documenting the persistent cybersecurity workforce shortage. Provides compelling data for justifying K-12 cybersecurity education programs and explaining why human-AI collaboration skills are increasingly valued by employers.

[\(ISC\)<sup>2</sup> Research](#)

## How to Use These Resources

### For Curriculum Development

Start with the **CYBER.org Standards** and **NICE Framework** to establish learning objectives, then draw on the pedagogical research to inform activity design.

### For Grant Writing

The workforce development references (Hoffman et al., ISC<sup>2</sup> reports) provide evidence for program justification. The educational research supports methodology choices.

### For Theoretical Grounding

If you're writing about or presenting on these activities, the posthuman/collaboration literature (Adams & Thompson, Braidotti, Luckin & Cukurova) provides scholarly context for the human-AI partnership framing.

### For Practical Implementation

The hands-on learning resources (Catota et al., Mitnick & Simon) offer concrete guidance for structuring technology-based learning experiences.

#### Suggest a Resource

Know of a resource that should be included here? Contact [ryanstraight@arizona.edu](mailto:ryanstraight@arizona.edu) with your suggestion.