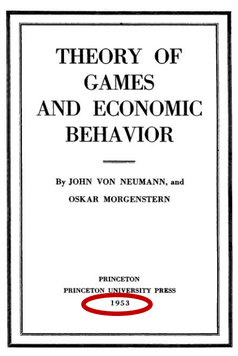
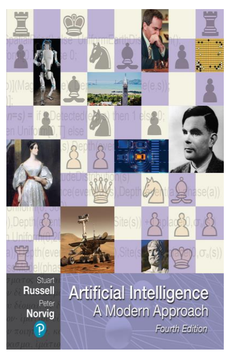
Advancing Cybersecurity Education to Human-Level Artificial Intelligence

PI: Fariborz Farahmand, Georgia Tech, fariborz@ece.gatech.edu

Challenges:

1) Simplifying Assumptions about Cybersecurity Behaviors



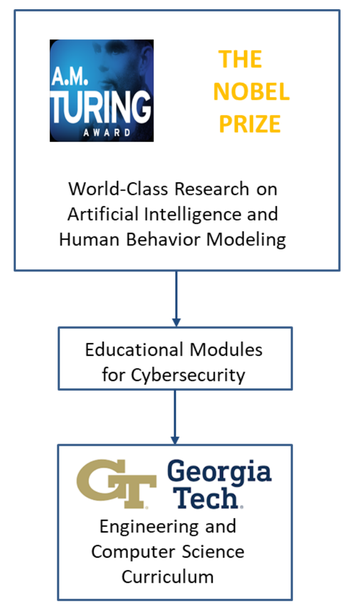


" A rational utility-based agent chooses the action that maximizes the expected utility of the action."

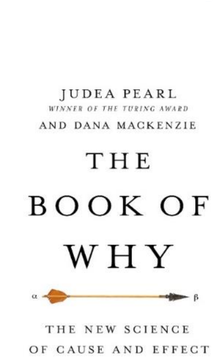
Solution:

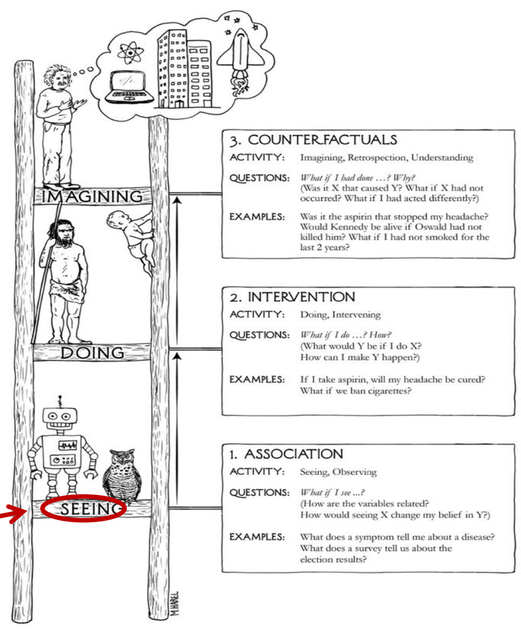
Integrate world-class research on artificial intelligence and human behavior modeling in educational modules:

- Provide thorough understanding of cybersecurity behaviors
- Learn causal (vs. association) relations from data
- Assess student learning



2) Learning Superficial Description of Reality





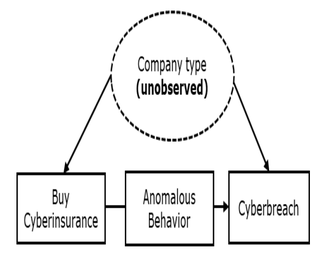
Artificial intelligence and cybersecurity are mostly here

Example- Applying Rules of *do*-Calculus to Assess Probability of Experiencing a Cyber Breach Given We Purchase Cyberinsurance

Query with *do*(.) operator

$$P(C|do(B)) = \sum_A P(C|do(B)),A)P(A|do(B)) \quad \text{Probability Axioms}$$
$$= \sum_A P(C|do(B)),do(A))\ P(A|do(B)) \quad \text{Rule 2}$$
$$= \sum_A P(C|do(B)),do(A))\ P(A|B) \quad \text{Rule 2}$$
$$= \sum_A P(C|do(A))\ P(A|B) \quad \text{Rule 3}$$
$$= \sum_{B'} \sum_A P(C|do(A),B')P(B'|do(A))P(A|B) \quad \text{Probability Axioms}$$
$$= \sum_{B'} \sum_A P(C|A,B')P(B'|\ do(A))P(A|B) \quad \text{Rule 2}$$
$$= \sum_{B'} \sum_A P(C|A,B')\ P(B')P(A|B) \quad \text{Rule 3}$$

Estimated answer without *do*(.) operator



Initial Results of First Module:

- 67 (of 91) students, with no background in cybersecurity and artificial intelligence, voluntarily completed the homework
- Gender did not make a significant difference in the students' performance, according to Mann–Whitney U test
- Module viewed 4,288 minutes, according to Canvas Analytics
- All students reached level 4 and 53 percent reached levels 5 and 6 of the cognitive domain in the canonical taxonomy of Bloom

Scientific Impact:

- Integrate world-class research on artificial intelligence and human behavior modeling in cybersecurity
- Prepare cybersecurity researchers who can develop realistic computational models of human behavior and untangle causation from correlation

Impact on Education & Outreach:

- Explain crosscutting cybersecurity concepts in a computational form
- Advance computational understanding of cybersecurity as a multifaceted domain

Impact on Broader Participation:

- Present common languages (e.g., *do*-calculus) to be spoken by engineers and computer scientists
- Facilitate interdisciplinary collaboration among cybersecurity, artificial intelligence, and cognitive science experts