National Nuclear Security Administration

United States
Department of Energy
National Nuclear Security Administration

International Nuclear Security

Artificial Intelligence Behavioral Recognition: Capabilities and Concerns

Justin Kinney

October 2025

ORNL-2025-245653

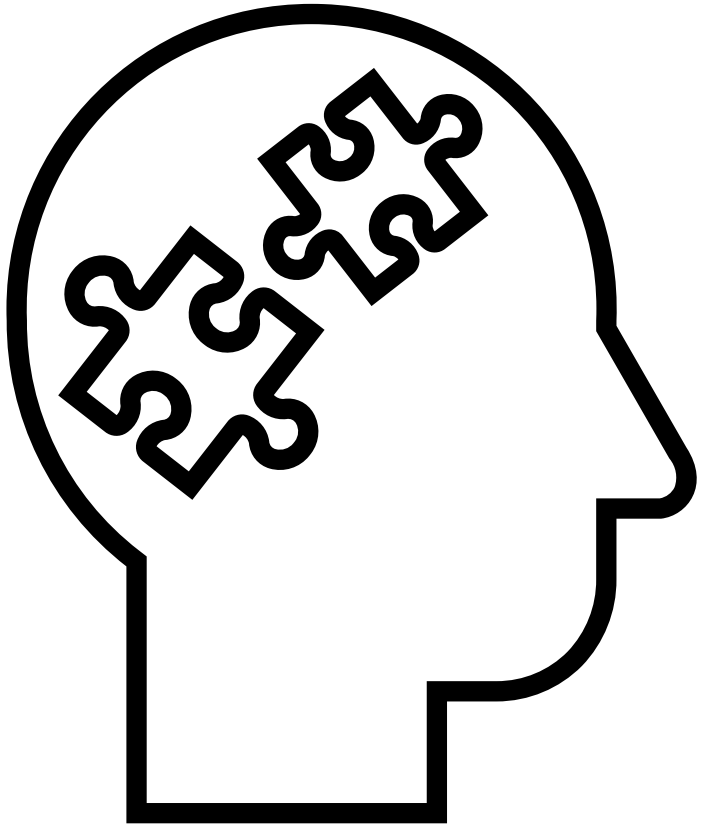
ORS Office of Radiological Security
Protect · Remove · Reduce

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

Learning Objectives

By the end of this session, you will be able to:

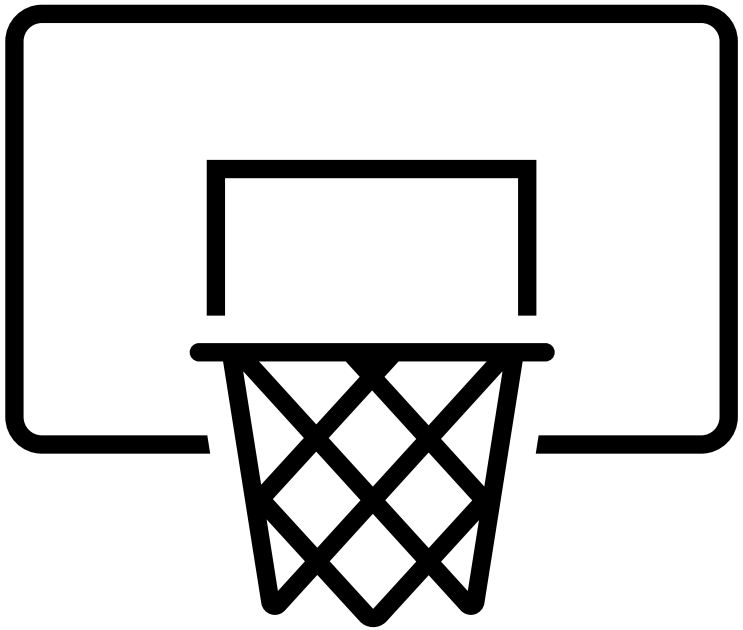
1. Define the term behavioral recognition.
2. Identify the ways that artificial intelligence and machine learning fit within behavioral analysis.
3. Identify different types of behavioral artificial intelligence and describe how it works.
4. Describe the challenges associated with implementing artificial intelligence in behavioral recognition.



What is behavioral recognition?

- The process of using technology to record, identify, and analyze patterns in human behavior
- Uses data from various sources to recognize patterns and identify deviations from those patterns
- Applications
  - Security
  - Healthcare
  - Customer Service

What is the goal of behavioral recognition?



- Seek to learn from complex, dynamic human interaction
- The goal is to detect anomalous or unusual behavior in a timely manner
- To react and adapt in real-time
- To use that information to mitigate any potentially harmful behavior
- To use that information to potentially predict future actions

How do Artificial Intelligence and Machine Learning Fit into Behavioral Recognition?

Artificial intelligence plays a growing role in behavioral analysis and cybersecurity

Capable of processing far more data than humans can manage alone.

Machine Learning helps train AI algorithms to identify patterns.

Algorithms trained with past and ongoing data collection to recognize normal versus abnormal behavior.

Learns and adapts in REAL-TIME

Dynamic performance improvement through machine learning over time.

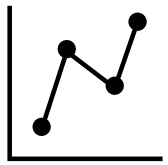
Combining Artificial Intelligence techniques with Behavioral Science

More timely detection of anomalies in large volumes of data

- Can process large quantities of data faster & scale up easily

More accurate detection

- Can recognize more subtle, nuanced deviation than humans



Contextual Analysis to detect evolving threats

- Provides increased context and additional for data & incorporating it into analysis

TYPES of Behavioral Artificial Intelligence

ANOMALY DETECTION

PREDICTIVE BEHAVIOR

REAL-TIME LEARNING

EMOTION-AWARE

So how does this work?

- **STEP ONE: Data Collection**
- **STEP TWO: Data Analysis**
- **STEP THREE: Application of Analysis**

1

STEP ONE

Data Collection

ORS Office of Radiological Security
Protect · Remove · Reduce

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

National Nuclear Security Administration

Data Collection

- Technical Data
  - Video surveillance
  - Computerized Tracking
  - Textual data interpretation
  - Sensor information

- Human Behavioral Data
  - Facial expressions and body language
  - Gait analysis
  - Tone
  - Computer behavior patterns

The AI algorithm is trained – the more input, the more accurate the data set. Using this data, the AI will formulate a “normal” baseline behavior pattern for comparison

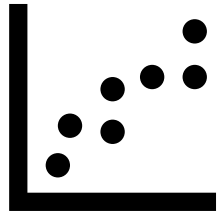
2

STEP TWO

Data Analysis

Data Analysis

- Machine Learning models process that collected data (both past collection and ongoing collection) through the trained algorithm
- Aggregation and Integration of multiple data streams



- Recognizes and categorizes patterns based on the input data – increasing accuracy with more input
- Ultimately seeks to identify pattern breaks – abnormal deviations from that baseline normal

2

STEP TWO

Data Analysis

ORS Office of Radiological Security
Protect · Remove · Reduce

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

National Nuclear Security Administration

Data Analysis (CONTINUED)

- Establishing a Behavioral Baseline
- Contextual Understanding
- Real-time adaptation – continuous learning models update with new input
- Delivers tailored insight and alerts to help users understand and respond to potential threats effectively

3

STEP THREE

Application

ORS Office of Radiological Security
Protect · Remove · Reduce

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

National Nuclear Security Administration

Analysis Application

- Trigger an alert when a deviation is detected – anything that breaks the established, trained pattern
- Provides insight into worker behavior
- Raise a “red flag” when anomalous behavior is detection
  - Unusual downloads, unauthorized access, unusual timing, detecting impairment, etc.

- <u>Still requires human oversight and validation!</u>

3

STEP THREE

Application

ORS Office of Radiological Security
Protect · Remove · Reduce

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

NNSA National Nuclear Security Administration

Application CONTINUED

- Identification of anomalies leads to identification of risk. AI can highlight deviations in employee behavior that *may* suggest risk
  - Detecting the Malicious Insider
    - Stress, aggression, purposeful deviation from the norm
  - Detecting the Unwitting Insider
    - Mistakes, negligence, accidental deviation from the norm
- Workplace Safety and Security
- Helps understand worker behavior
- Prediction – forecasting future behavior based on the historical data

The Importance of Human Oversight

Ultimately, Artificial Intelligence and Machine Learning still require a significant degree of oversight to be effective

They can detect an anomaly, but can't tell you if that anomaly is a concern

False positives are inevitable.

QUESTION: In highly-sensitive, high-consequence industries, you can't afford many mistakes. Who is accountable? Who holds responsibility for its decisions?

Challenges of AI in Behavioral Recognition

Accuracy

Privacy

Ethical Considerations

Computational Power

Overreliance Risk

Conclusion

Behavioral Recognition has great potential as a powerful tool in enhancing security.

Artificial intelligence provides real-time anomaly detection with faster response times than human-driven observation.

Handles large volumes of data, capable of scaling up with growing networks. Constantly learning and improving with new input data.

However, careful usage of AI tools is essential, as there are several practical and ethical considerations.