United States
Department of Energy
National Nuclear Security Administration
International Nuclear Security

Artificial Intelligence and Machine Learning – Emerging Technologies and Applications in Nuclear Security

M. Bertolli[1], E. Brayfindley[2], K. Dayman[3], T.Edmunds[4], S. Eggers[5], A. Hagen[2], J. Hite[3], A. Luttman[2,*], B. Phathanapirom[3], J. Preston[1], C. Sample[5], S. Stewart[3]

[1]Y-12 National Security Complex [2]Pacific Northwest National Laboratory [3]Oak Ridge National Laboratory [4]Lawrence Livermore National Laboratory [5]Idaho National Laboratory

February 1, 2024

PNNL-SA-164261

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

Emergence and Applications of AI/ML to Nuclear Security

- Artificial intelligence and machine learning (AI/ML) is an emerging technology impacting nearly all industries, including:
  - Safeguards
  - Nuclear Security and Physical Protection
  - Material Control and Accounting
  - Nonproliferation
- Focus use cases for this presentation:
  - AI/ML-enabled Data Fusion
  - Automated Social Engineering
  - Digital Data Vulnerabilities and Protections

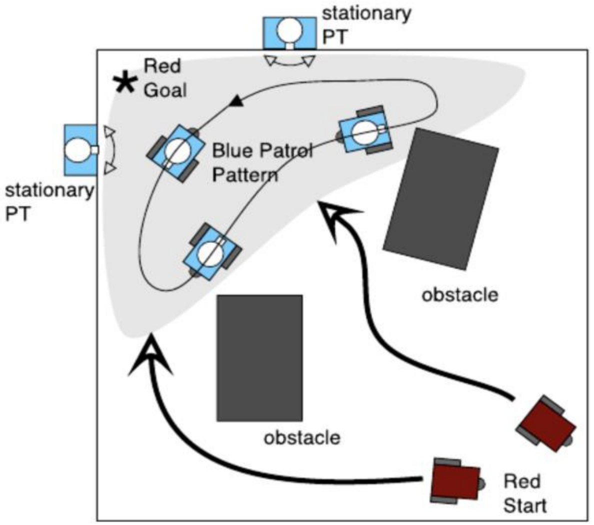
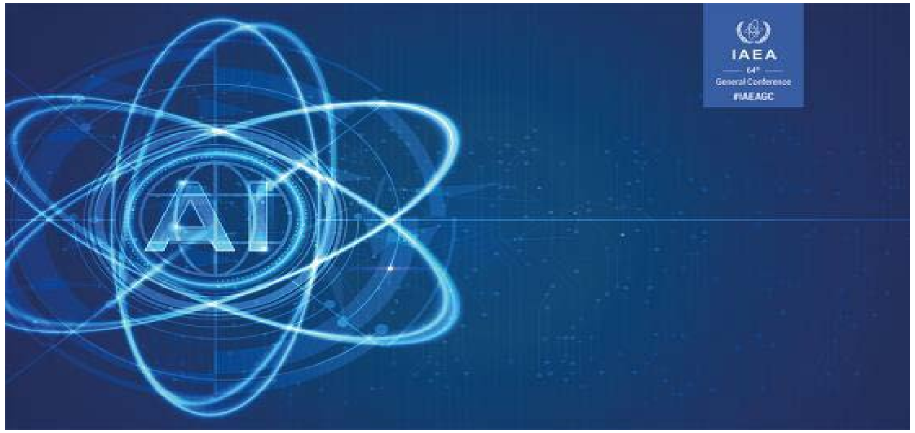


Image from Thorton, et al, Computational Intelligence, 2015.

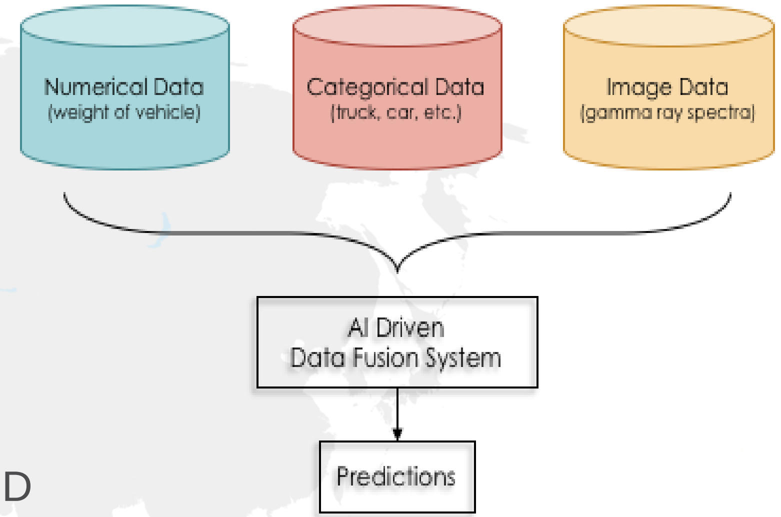


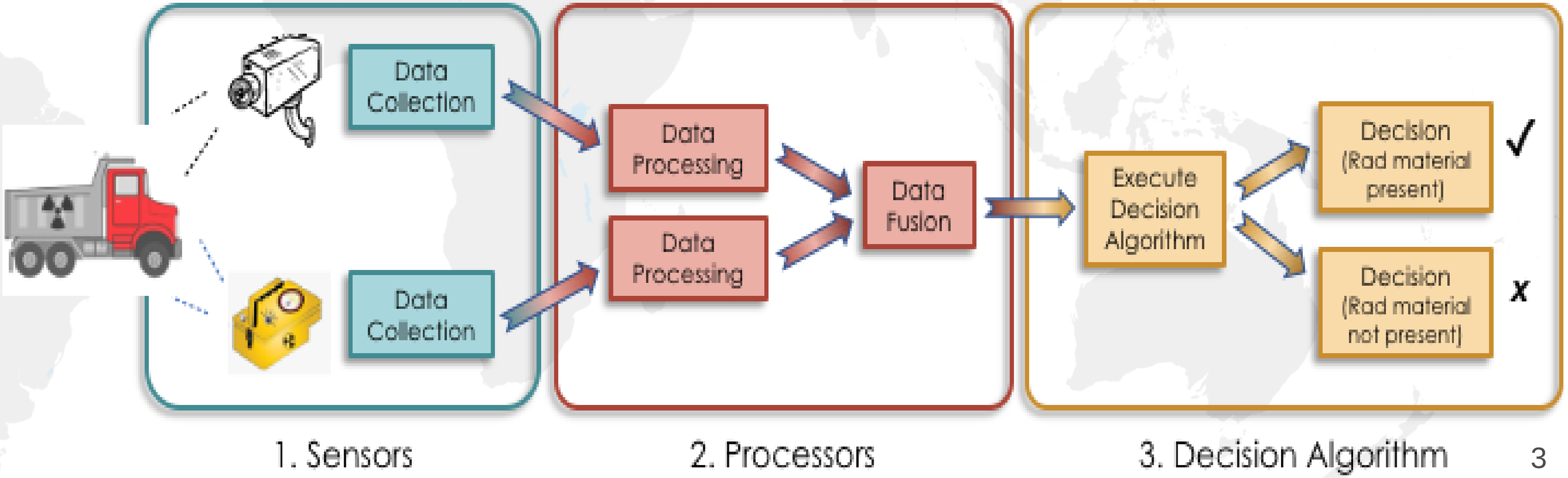
AI/ML-enabled Data Fusion in Nuclear Security

Data fusion: Synergistic, automated integration of sensory inputs (data)

Exemplar Data Fusion Nuclear Security Applications

- Automation of Material Control & Accounting Tasks
  - Fusing measurements of radioactivity, weight, container RFID
- Improved Tracking of People and Material Movements
  - Fusing badge reader information with security camera imagery or container RFID
- Transportation Security
  - Enhanced vehicle ID and tracking
- Perimeter Intrusion and Detection Systems





AI for Social Engineering

Social Engineering: “Any act that influences a person to take an action that may or may not be in their best interest.”*

Examples of social engineering tactics and where AI/ML comes into play:

- Baiting
- Phishing
- Spear Phishing
- Vishing
- Pretexting
- Scareware
- Quid Pro Quo
- Diversion Theft
- Tailgating

Attackers go for the low-hanging fruit: *humans*
Email
Social Media and Internet
Trends
Criminal Groups
Attack vectors

*Christopher Hadnagy. 2018. *Social Engineering: The Science of Human Hacking*. 2nd ed. Hoboken, NJ: Wiley Publishing.

AI for Social Engineering

Social Engineering: “Any act that influences a person to take an action that may or may not be in their best interest”*

Examples of social engineering tactics and where AI/ML comes into play:

- Baiting
- Phishing
- Spear Phishing
- Vishing
- Pretexting
- Scareware
- Quid Pro Quo
- Diversion Theft
- Tailgating

Directly Enhanced with AI/ML

Attackers go for the low-hanging fruit: *humans*
Email
Social Media and Internet
Trends
Criminal Groups
Attack vectors

*Christopher Hadnagy. 2018. *Social Engineering: The Science of Human Hacking*. 2nd ed. Hoboken, NJ: Wiley Publishing.

AI for Social Engineering

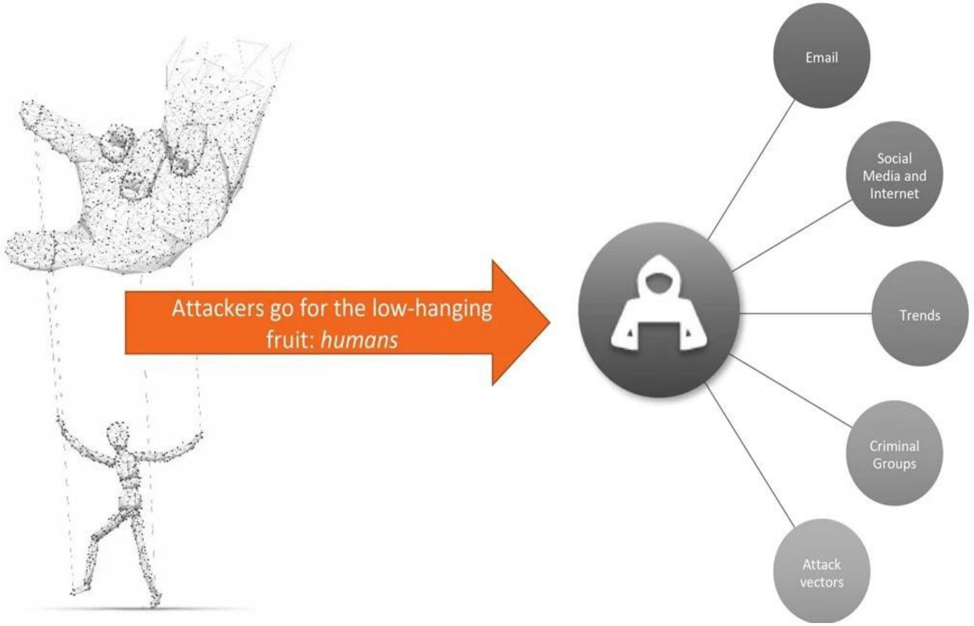
Social Engineering: “Any act that influences a person to take an action that may or may not be in their best interest”*

Examples of social engineering tactics and where AI/ML comes into play:

- Baiting
- Phishing
- Spear Phishing
- Vishing
- Pretexting
- Scareware

- Quid Pro Quo
- Diversion Theft
- Tailgating

Indirectly Enhanced with AI/ML; usually data mining


Attackers go for the low-hanging fruit: *humans*
Email
Social Media and Internet
Trends
Criminal Groups
Attack vectors

Christopher Hadnagy. 2018. *Social Engineering: The Science of Human Hacking*. 2nd ed. Hoboken, NJ: Wiley Publishing.

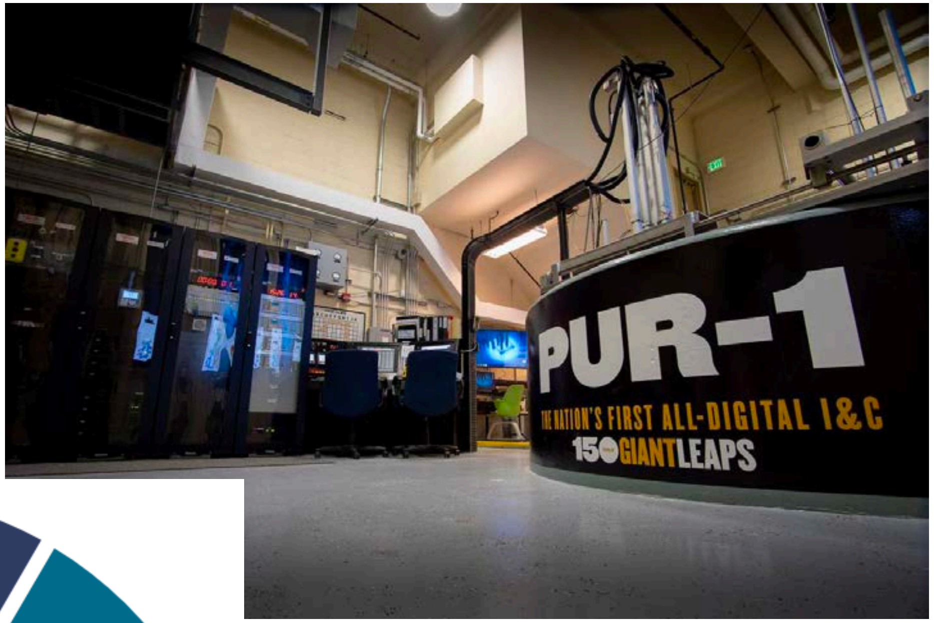
AI for Social Engineering – Example: Operations/Mechanisms

- Information Aggregation
  - Information Brokers
  - Social Media
- Supply Chain Vulnerabilities
- Content Generation
  - Deepfakes
  - Language Generation and Manipulation
- Content Ingestion
  - Malware
  - Filter Bubbles

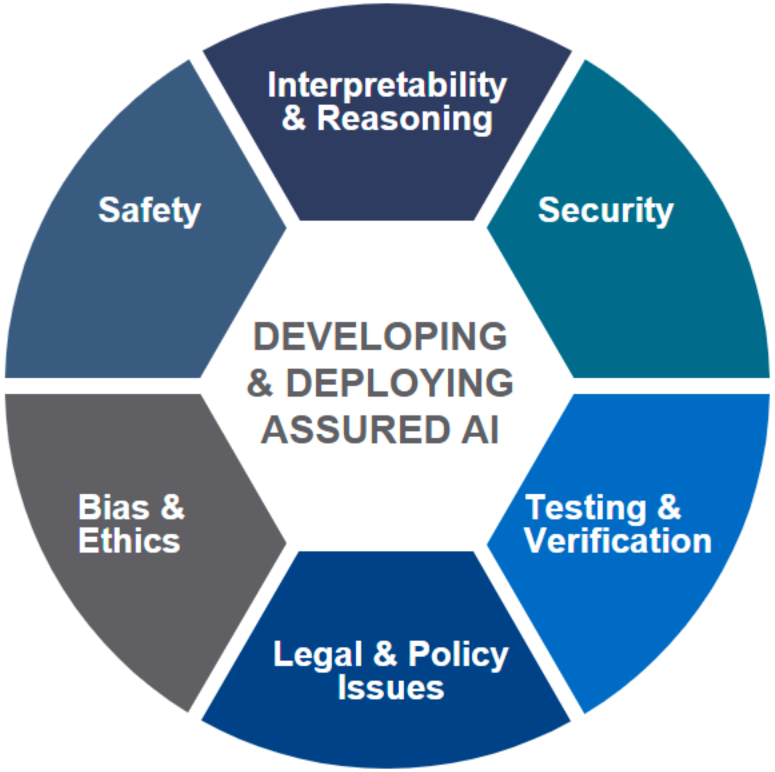
https://www.newsweek.com/tom-cruise-deepfake-tiktok-new-1594525

Digital Data Vulnerabilities and Protections

- AI/ML is different from other software and models:
  - Distinct software lifecycles
  - Driven by (usually large) amounts of data
  - Data and model architectures often downloaded from internet
- So it
  - Has different vulnerabilities
  - Requires different protections
  - Benefits from international cooperation on policy



https://www.purdue.edu/newsroom/releases/2019/Q3/first-all-digital-nuclear-reactor-control-system-in-the-u.s.-installed-at-purdue-university.html



INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

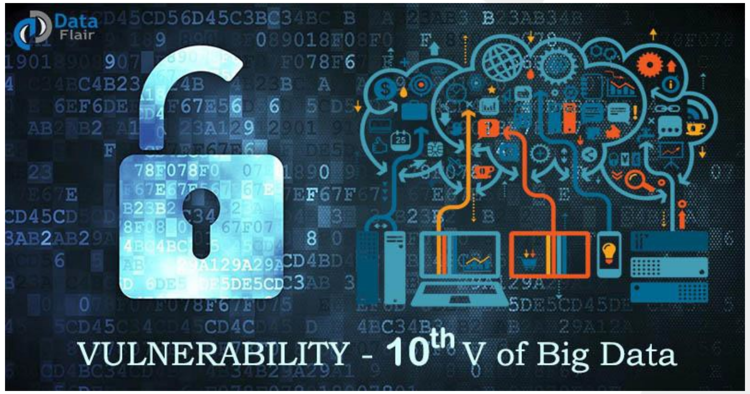
Digital Data Vulnerabilities and Protections

All AI is Built on Data

- Data Types
- Data Vulnerabilities
  - Open Source
  - AI Application Models
  - AI Training and Operations

Data Type	Description
Endpoint	Operational or security-related information generated by ICT, OT, or industrial internet of things edge devices, such as sensors, programmable logic controllers, cameras, or computers
Communication	Generated as part of the network transmission process
Configuration	Settings in ICT, OT, or industrial internet of things devices
Monitoring	Generated during monitoring activities, such as system logs, alerts, and indications
Metadata	Describes other data

OSINT Example	Potential Adversarial Misuse
Facility layout and hardware, software, and firmware design information for digital systems and ICT or OT architectures	Enables development of physical, cyber, or hybrid attacks against the facility infrastructure and systems
Type, quantity, quality, and location of nuclear material or radioactive material	Enables theft of nuclear or radioactive material
Sensitive transport information, such as schedules, routes, and vehicles	Enables theft of nuclear or radioactive material
Personnel information, including phone numbers, email addresses, and work location	Identifies targets for social engineering campaigns



INS International Nuclear Security

Reducing Risk of Nuclear Terrorism