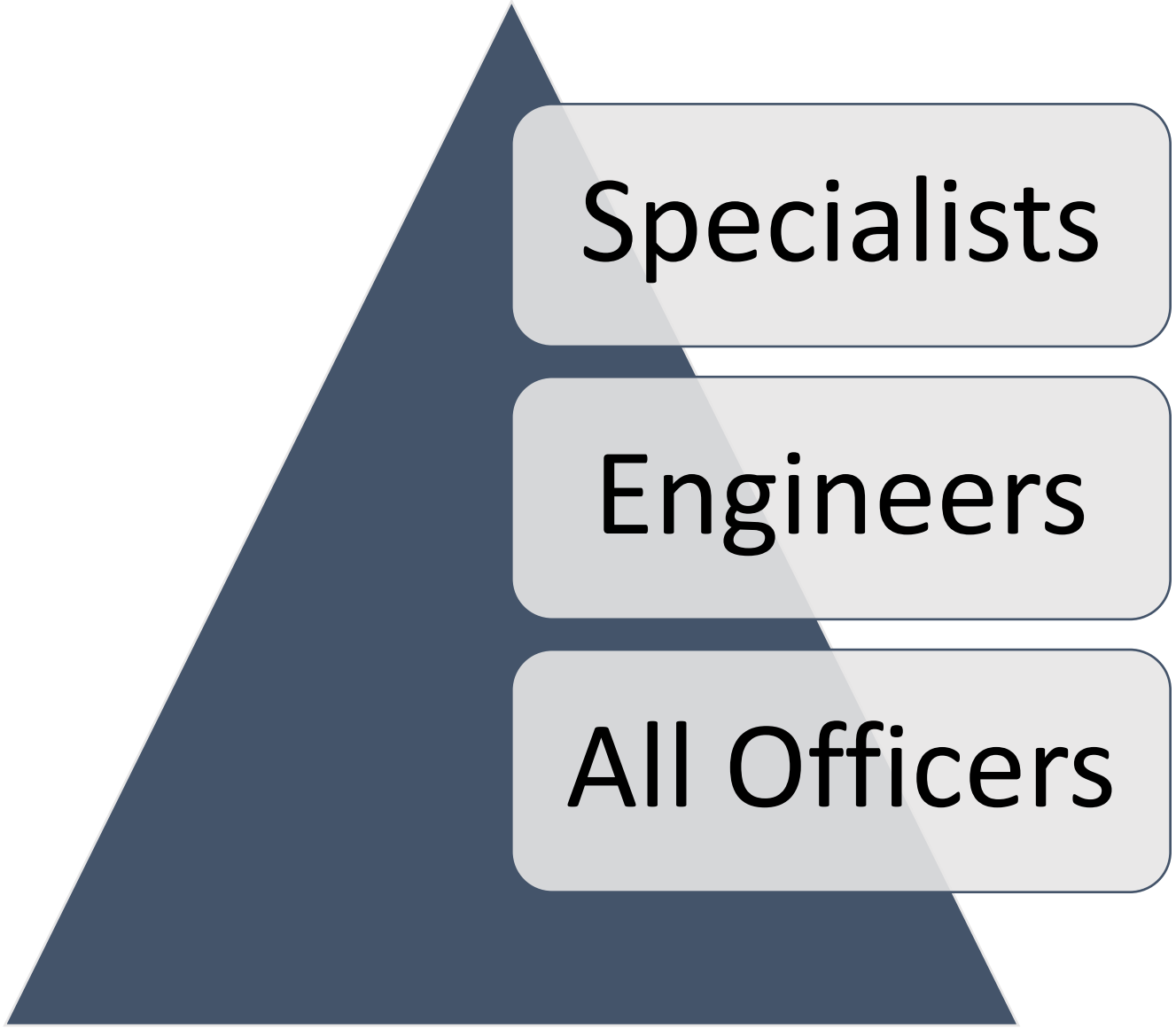
EUMACS Seminar: AI and Cyber

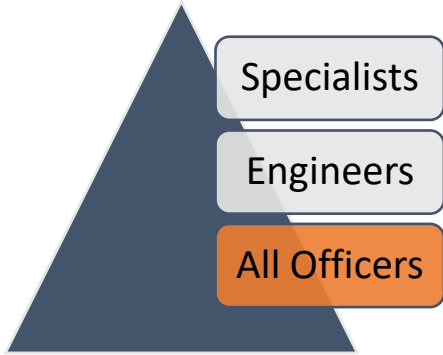
Wim Mees
Filip Van Utterbeeck

06 June 2024

3 levels of learning about AI and Cyber



Possible “AI Literacy” course outcomes

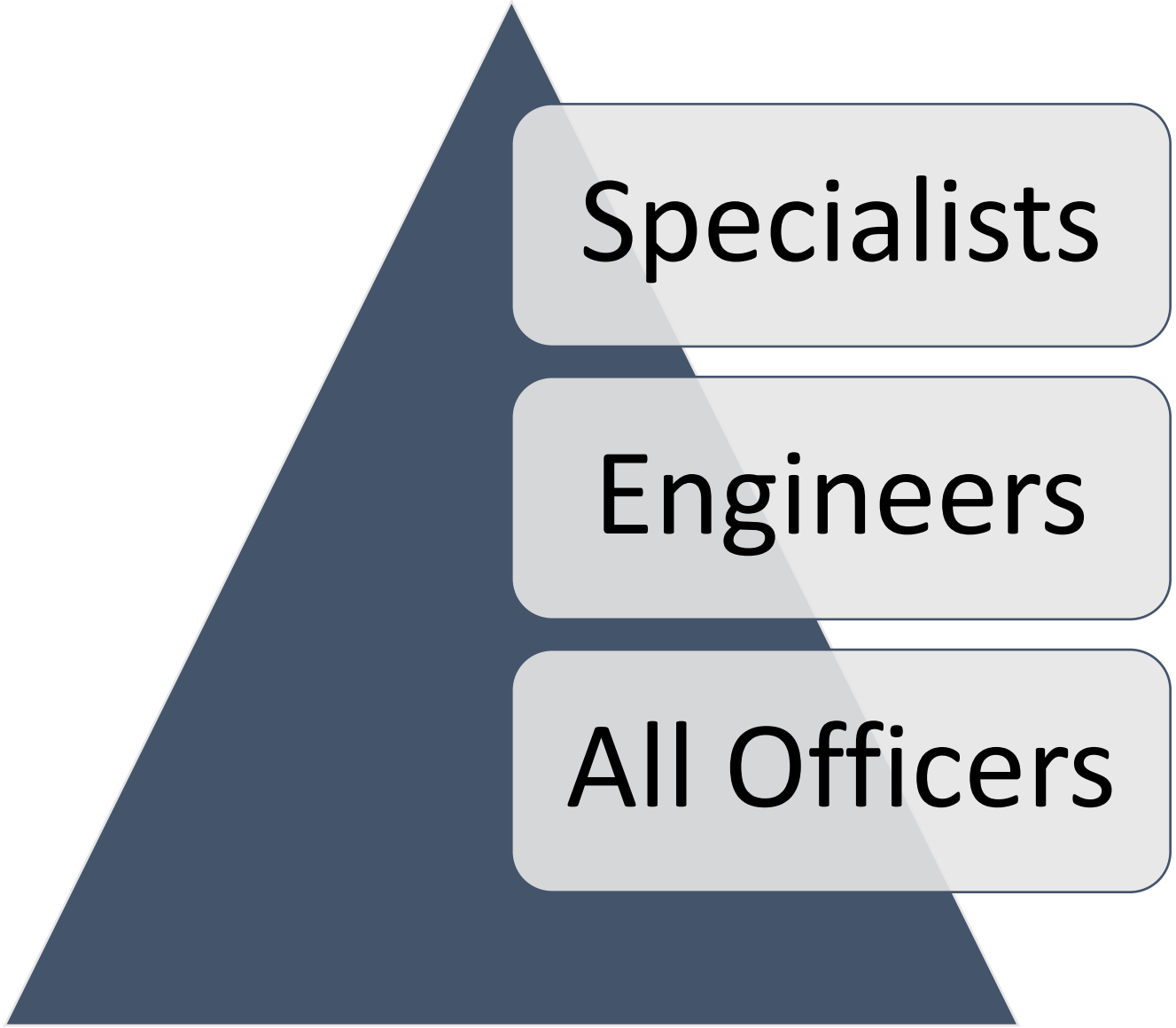


- Understand the basic concepts and types of AI
- Military applications of AI
- Utilize AI tools (like ChatGPT) effectively for various applications
- Recognize the limitations and potential risks associated with AI
- Reflect on the ethical, legal and societal implications of AI use
- Reflect on best practices for responsible AI usage in a defence context

Cybersecurity

- All officers:
  general cyber awareness
  - Part of professional training, not an academic course
  - Role of CyCom ?

3 levels of learning about AI and Cyber



Cybersecurity NIST

National Initiative for Cybersecurity Education (NICE)

Workforce Categories

Specialty Areas

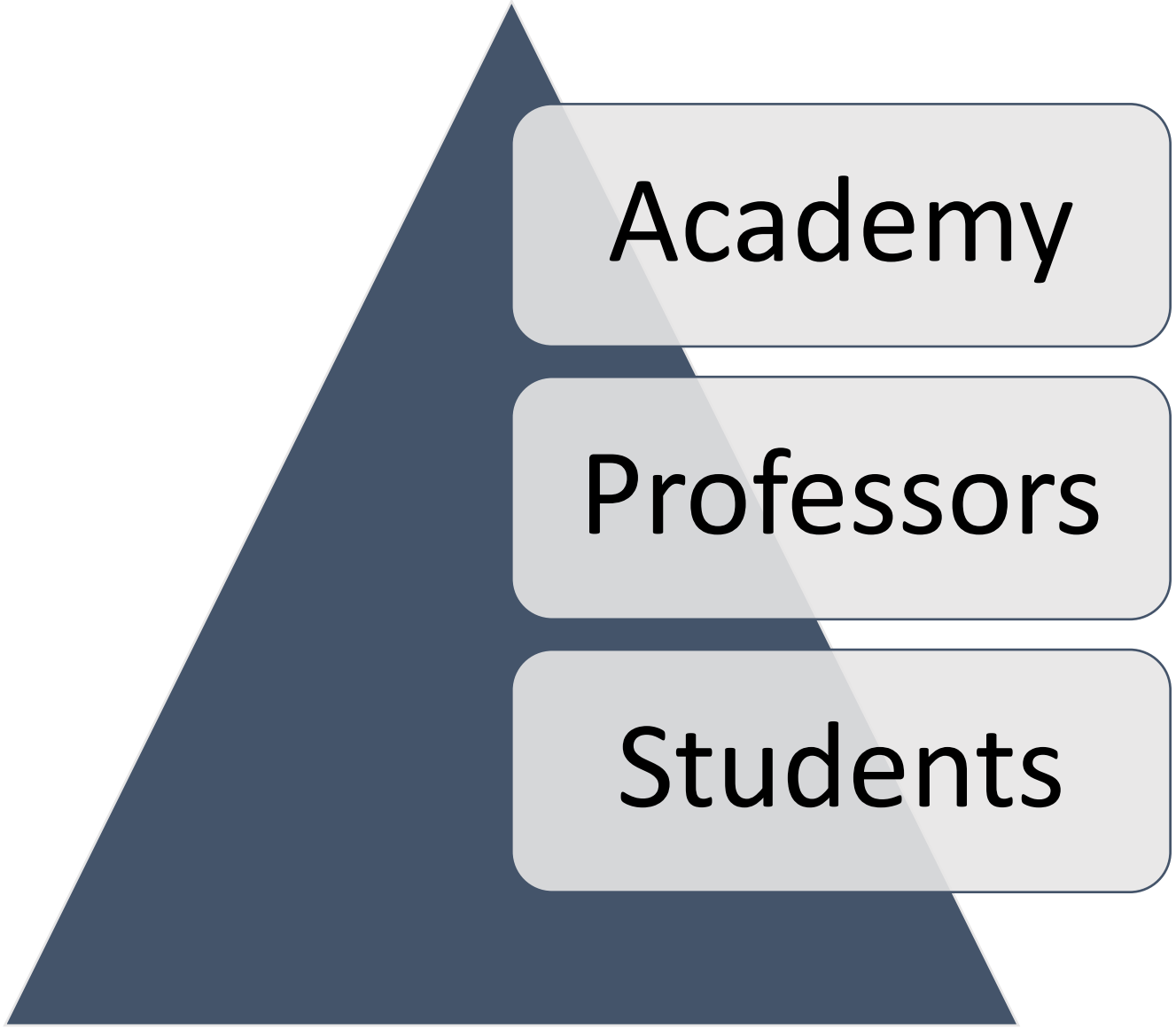
Securely Provision	Operate & Maintain	Oversee & Govern	Protect & Defend	Analyze	Collect & Operate	Investigate
Risk Management	Data Administration	Legal Advice & Advocacy	Cybersecurity Defense Analysis	Threat Analysis	Collection Operations	Cyber Investigation
Software Development	Knowledge Management	Training Education and Awareness	Cybersecurity Defense Infr Analysis	Exploitation Analysis	Cyber Operations Planning	Digital Forensics
Systems Architecture	Customer Service & Tech Support	Cybersecurity Management	Incident Response	All-Source Analysis	Cyber Operations	
Technology R&D	Network Services	Strategic Planning & Policy	Vulnerability Assessment & Management	Targets		
Systems Requirements Planning	Systems Administration	Executive Cyber Leadership		Language Analysis		
Test & Evaluation	Systems Analysis	Program/Project Management & Acquisition				
Systems Development						

Organizes **Work Roles** into **Categories** & **Specialty Areas**

Defines **Knowledge Skills Abilities (KSAs)**

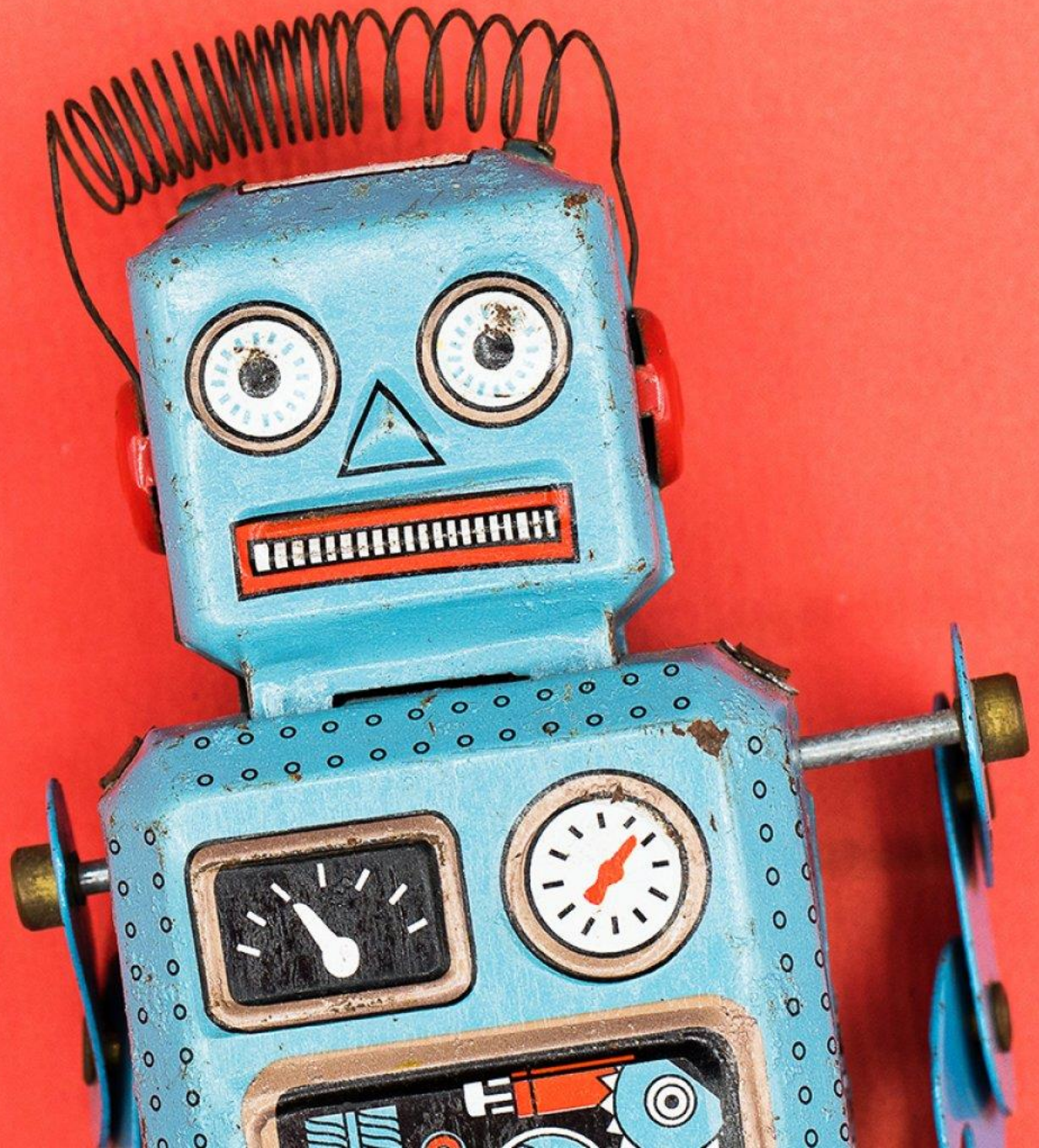
Associates **Tasks**

3 levels of learning with AI

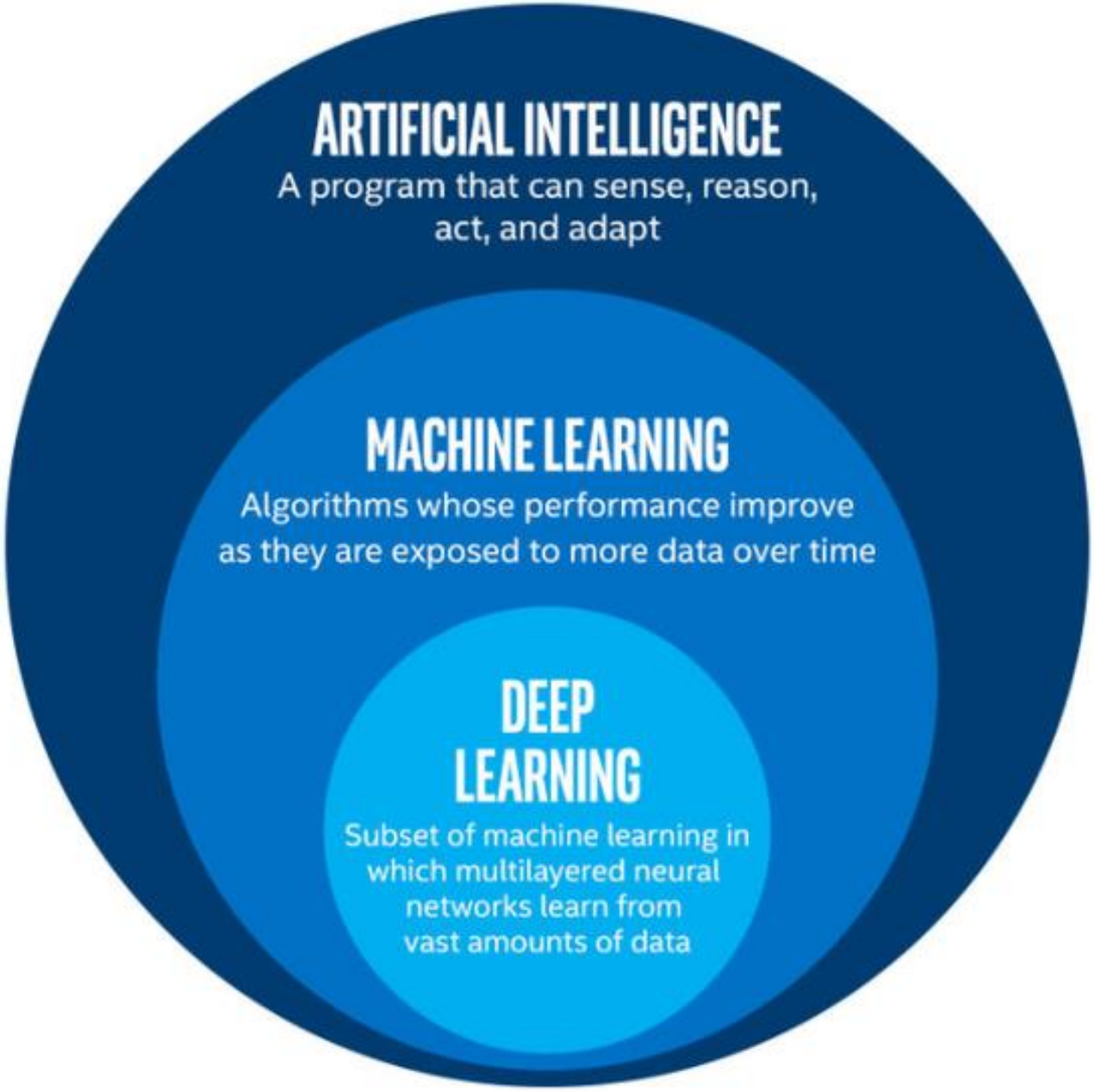


Take-aways

- “literacy” in these fields crucial for ALL officers
  - Not only engineering, also including legal and ethical aspects
- Fast evolving fields -> courses must adapt
- Priority for several nations, specialized personnel crucial
  - In-house vs partnership civilian universities
- “Train the teachers” about AI (partnership civilian universities)



3 levels of AI



Specialists

Engineers

All Officers

Example course from RMA

DS425: Intelligent Decision Making Methods

Introduction to AI

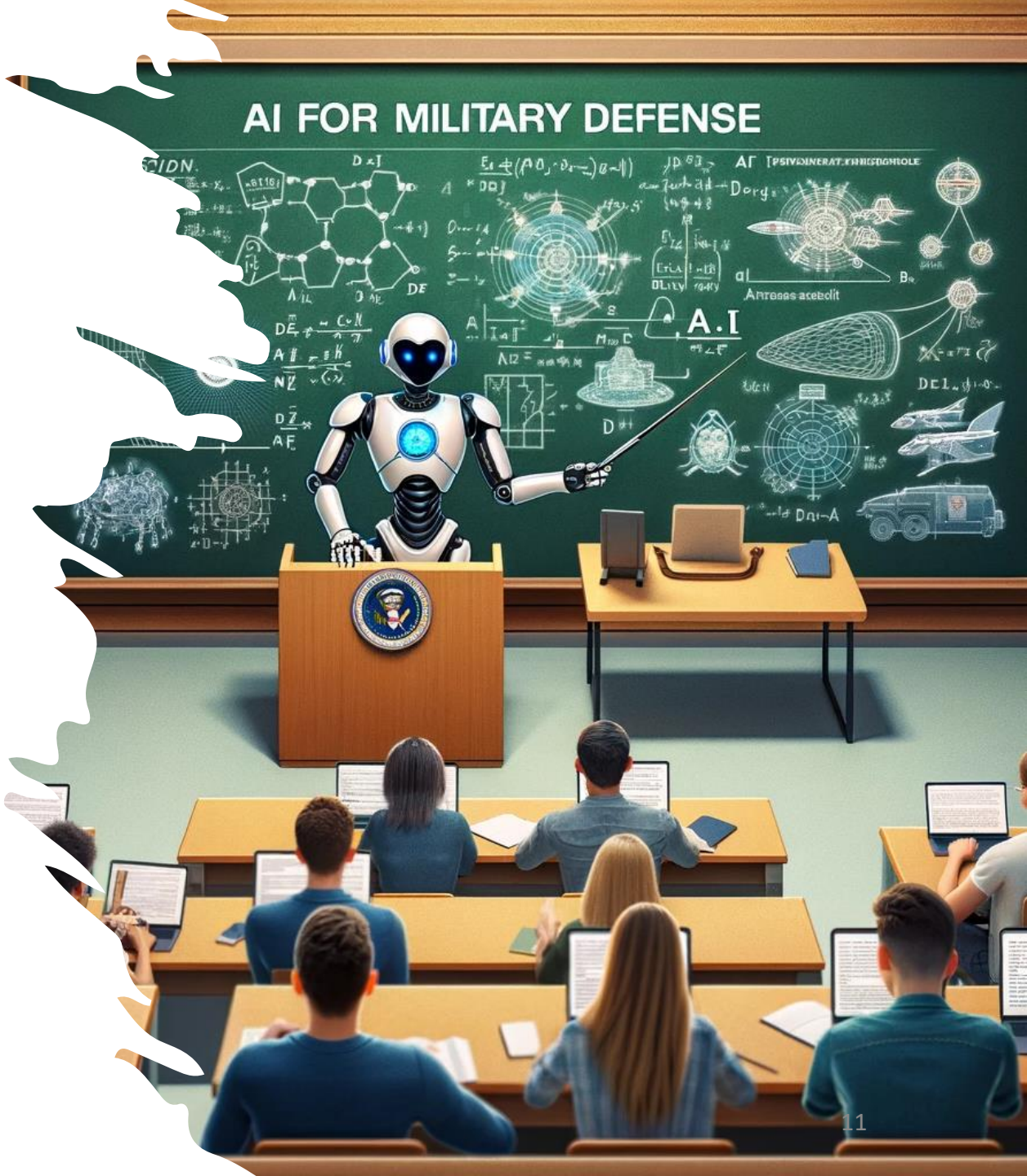
Part 1: Search and decision making

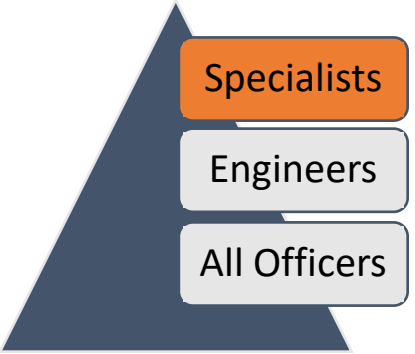
- Tree search (uninformed/informed)
- Local Search
- Adverserial Search
- Constraint Satisfaction Problems

Part 2: Machine learning

- Supervised learning (classical methods/deep learning)
- Unsupervised learning
- Applications in Natural Language Processing
- Reinforcement learning

Research project





Building blocks for specialized AI semesters

History of AI	Search Algorithms	Knowledge representation and reasoning	Machine Learning Basics	Neural Networks and Deep Learning
Natural Language Processing	Computer Vision	Robotics	Reinforcement Learning	Legal and Ethical aspects in AI
Uncertainty and Probabilistic AI Models	Big Data and Privacy	Speech Recognition	Multi-Agent Systems	…

STUDENT-FOCUSED AIED
Intelligent Tutoring Systems (ITS)
AI-assisted Apps (e.g., maths, text-to-speech, language learning)
AI-assisted Simulations (e.g., games-based learning, VR, AR)
AI to Support Learners with Disabilities
Automatic Essay Writing (AEW)
Chatbots
Automatic Formative Assessment (AFA)
Learning Network Orchestrators
Dialogue-based Tutoring Systems (DBTS)
Exploratory Learning Environments (ELE)
AI-assisted Lifelong Learning Assistant
TEACHER-FOCUSED AIED
Plagiarism detection
Smart Curation of Learning Materials
Classroom Monitoring
Automatic Summative Assessment
AI Teaching Assistant (including assessment assistant)
Classroom Orchestration
INSTITUTION-FOCUSED AIED
Admissions (e.g., student selection)
Course-planning, Scheduling, Timetabling
School Security
Identifying *Dropouts* and *Students at risk*
e-Proctoring

Holmes, W., & Tuomi, I. (2022). State of the art and practice in AI in education. European Journal of Education, 57(4), 542-570

Cybersecurity

- All officers
  - General cyber awareness
- Engineers / Tech officers
  - Securely provision C4ISR systems
  - Operate & Maintain
  - Oversee & Govern
- Specialists
  - Protect & Defend
  - Analyze threats & Respond to incidents
  - Investigate incidents

Cybersecurity ENISA

Cybersecurity NIST

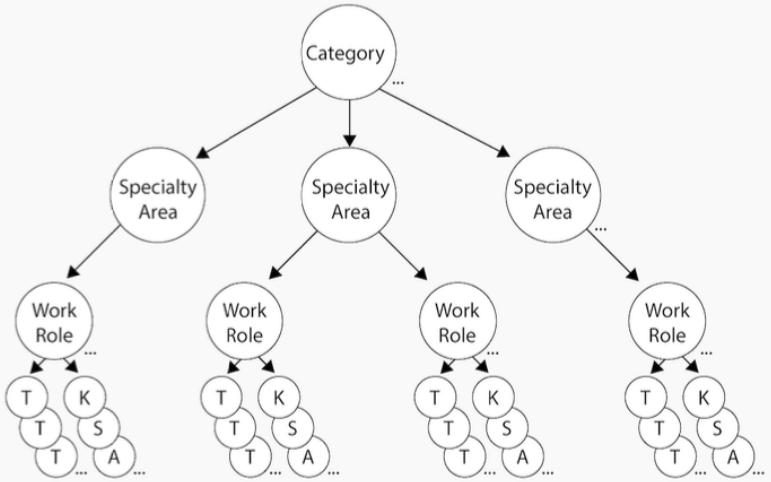
WHAT IS THE CYBERSECURITY WORKFORCE?

A workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations.

CATEGORIES: A high-level grouping of common cybersecurity functions

SPECIALTY AREAS: Represent an area of concentrated work, or function, within cybersecurity and related work

WORK ROLES: The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role



TASKS: Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

KSAs: Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Cybersecurity SANS

Securely Provision (SP)

Specialty Area: Software Development (DEV)
Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

Work Role: Secure Software Developer (SP-DEV-001)
Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

SANS Training Course	GIAC Certification	Work Role Proficiency
DEV522: Defending Web Applications Security Essentials	GWEB: GIAC Certified Web Application Defender	3: Advanced
SEC540: Cloud Security and DevOps Automation	GCSA: GIAC Cloud Security Automation	3: Advanced

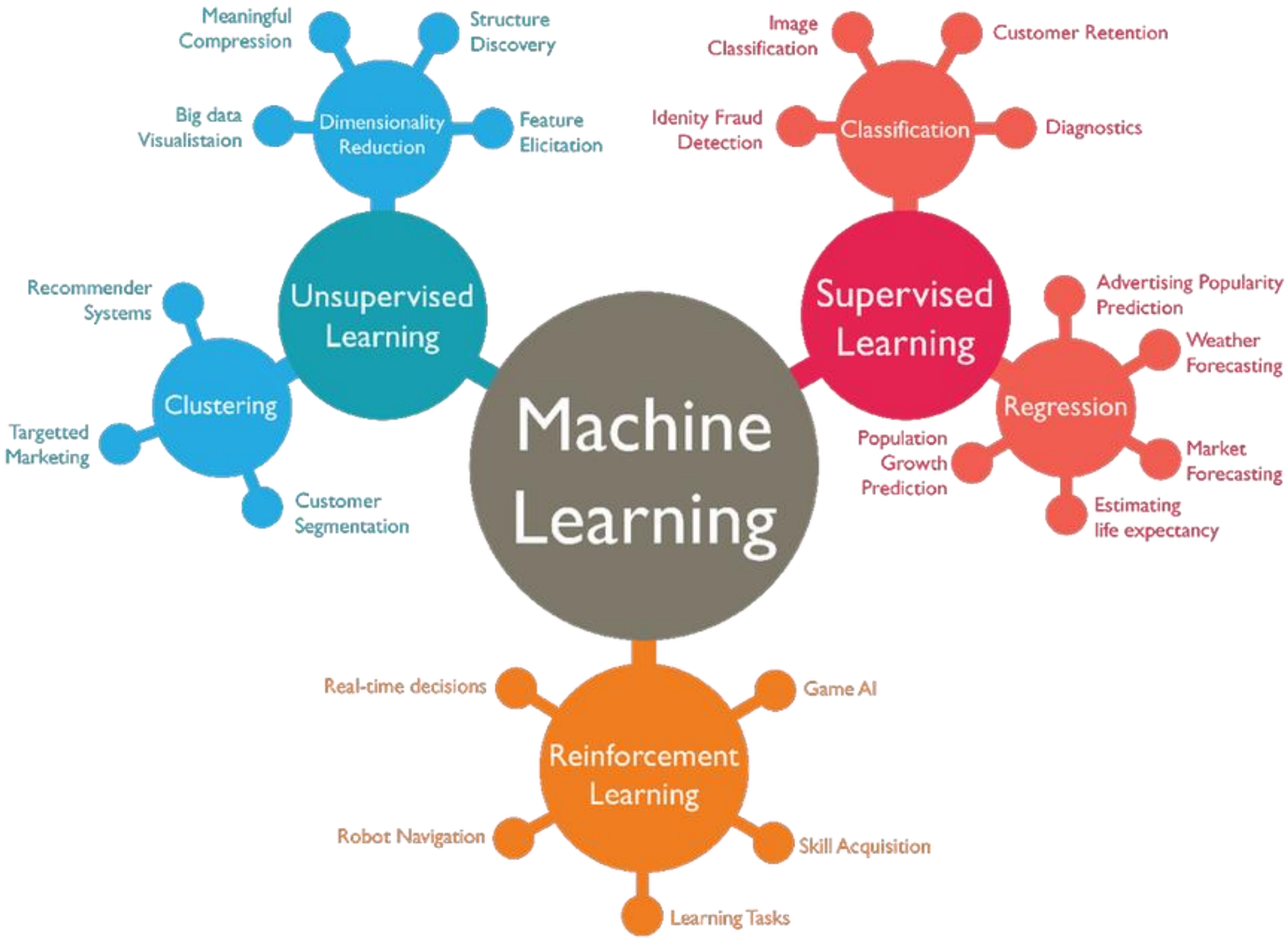
Other Mapped SANS Training and GIAC Certifications:
SEC505: Securing Windows and PowerShell Automation / GCWN: GIAC Certified Windows Security Administrator
SEC506: Securing Linux/Unix / GCUX: GIAC Certified Unix Security Administrator
DEV534: Secure DevOps: A Practical Introduction
SEC573: Automating Information Security with Python / GPYC: GIAC Python Coder

Cybersecurity RMA

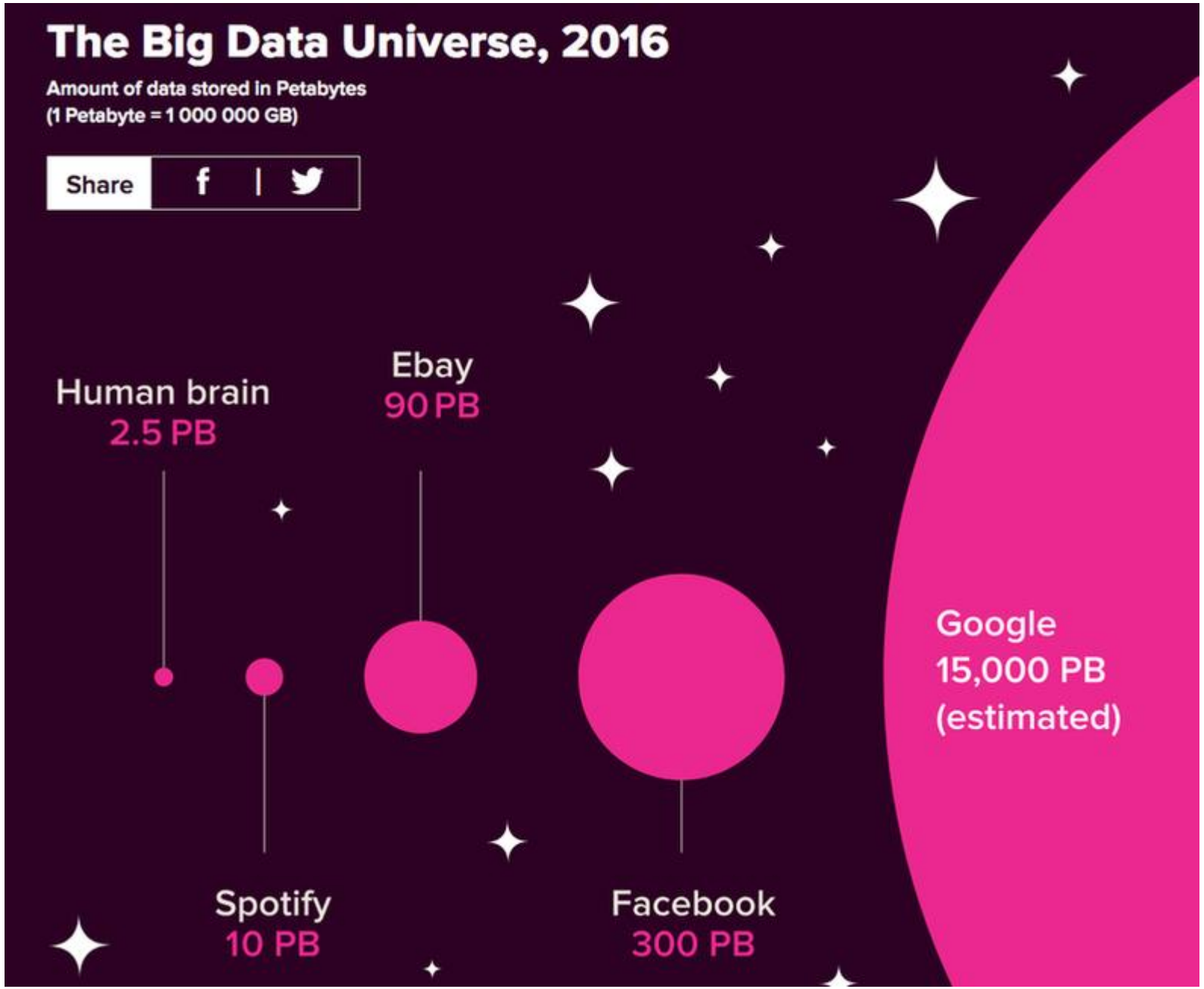
- BaMa SSMW
  - Not technology oriented
  - Limited specialization in Ma with 1 Cyber course
- BaMa POL
  - Technology/Engineering oriented
  - Specialization “Network Enabled Capabilities” (NEC)
  - Multiple cyber courses (management of cybersecurity, network security, forensics, malware reverse engineering)
- Ma Cyber (inter-university)
  - 120 ECTS shared cybersecurity curriculum (includes the RMA courses)
  - Not part of RMA curriculum but free admission for RMA students

Cybersecurity

- Challenging field: rapidly evolving, complex, …
- Example: cybersecurity of AI (LLM) systems
  - Input validation: from basic fields to complex prompts
  - Supply chain: from software supply chain to “training data, models, augmentation sources (RAG), and software” supply chain
  - Least privilege: from fine-grained ABAC/RBAC/MAC/DAC to the LLM has access to the full datastore
  - Shift left: from convincing software engineers to “educating” data scientist
  - Etc.
- Curriculum must evolve frequently and must be supported by scientific research and SMEs


Machine Learning
Unsupervised Learning
Dimensionality Reduction
Meaningful Compression
Structure Discovery
Big data Visualistaion
Feature Elicitation
Clustering
Recommender Systems
Targetted Marketing
Customer Segmentation
Supervised Learning
Classification
Image Classification
Customer Retention
Idenity Fraud Detection
Diagnostics
Regression
Advertising Popularity Prediction
Weather Forecasting
Population Growth Prediction
Market Forecasting
Estimating life expectancy
Reinforcement Learning
Real-time decisions
Game AI
Robot Navigation
Skill Acquisition
Learning Tasks

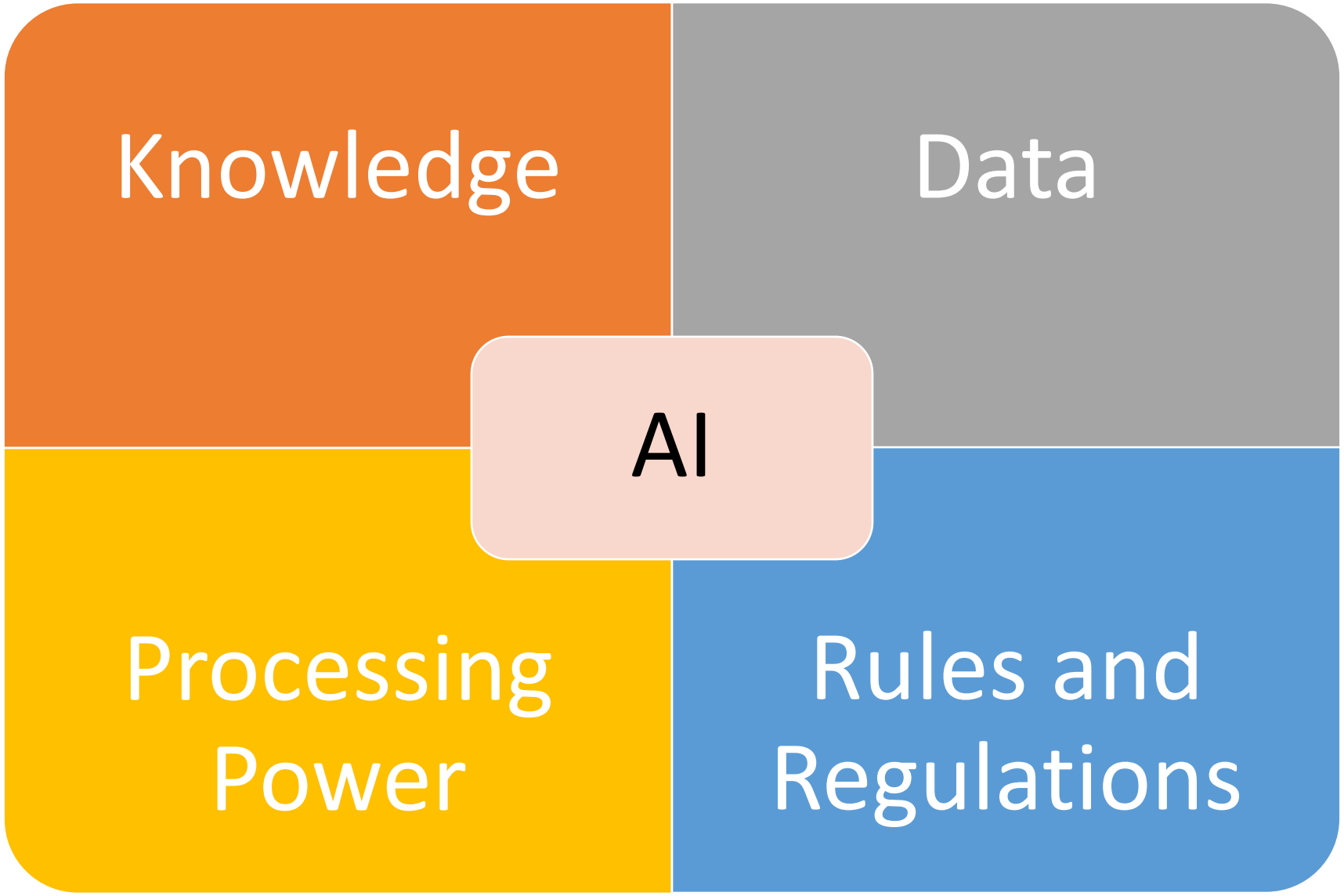
Generative AI and Artificial Creativity



Data

1990 internet traffic:
100 GB/day

2017 internet traffic:
45000 GB/second


Knowledge
Data
AI
Processing Power
Rules and Regulations


WSJ

Generative AI and Artificial Creativity

- Possible military applications
  - Deepfake creation and detection
  - Narrative generation
    - E.g. enhanced situational awareness based on reports (potentially from autonomous devices)
    - Automated reports/orders
    - Proposing alternative COAs
    - Generation of training content (video, image, text)
  - NLP
    - Machine translation, summarization (from text or audio), sentiment analysis
    - Question answering systems/chatbots

Game playing: intelligent decision making

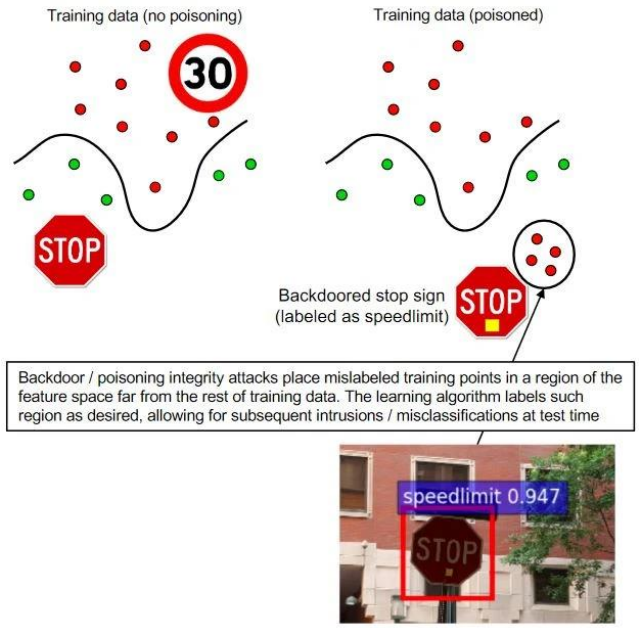
- Possible military applications
  - AI-enabled wargaming
  - Managing fleets of autonomous vehicles
  - Decision-making assistance
    - Strategic planning
    - Recommendations for COA

Image understanding

- State of the art
  - Deep learning for image recognition has become more or less “routine”…if training data available
  - Image captioning and visual question answering remain more difficult

- Possible military applications
  - Surveillance of large areas
  - Target recognition
  - Individual targeted surveillance

- Challenges
  - Ethical/Legal implications
  - Adversarial AI



Robotics

- State of the art
  - Self-driving cars remain around the corner
  - Advanced robots performing acrobatics actually not based on AI but control theory
  - Unmanned autonomous systems
- Possible military applications
  - UAS
  - Logistics/resupply
- Challenges
  - Ethical/Legal implications