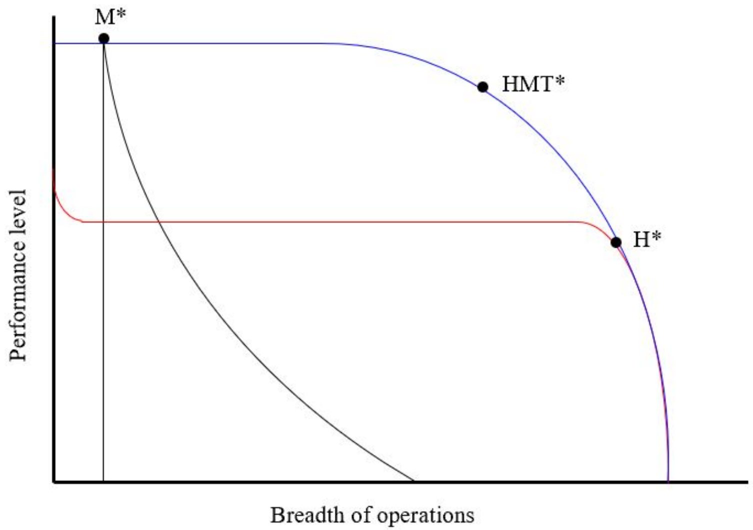
HUMAN-MACHINE TEAMING

MATT GENTZEL. LEO KLENNER. ROB WIMBERLY. JJ LEE.

Why HMT?

> Comparative advantage of human and machine performance characteristics

Performance Graph



> **Black** line represents the performance curve of a **machine** (M)
> **Red** line represents the performance curve of a **human** (H)
> **Blue** line represents the performance curve a **human-machine team** (HMT)

Conceptualizing HMT Alternatives

> HMT can take places during both the **deployment** and the **development** phases of a machine

> The deployment phase is shaped by **horizontal alternatives** to HMT, e.g. should we deploy a manned system or a manned-unmanned team?

> The development phase is shaped by **vertical alternatives** inside HMT, e.g. what type of algorithms should we use to build the machine?

> Criteria for assessing these alternatives:

Dependence on human input	Degree of generative behavior	Execution capabilities	Robustness	Predictability

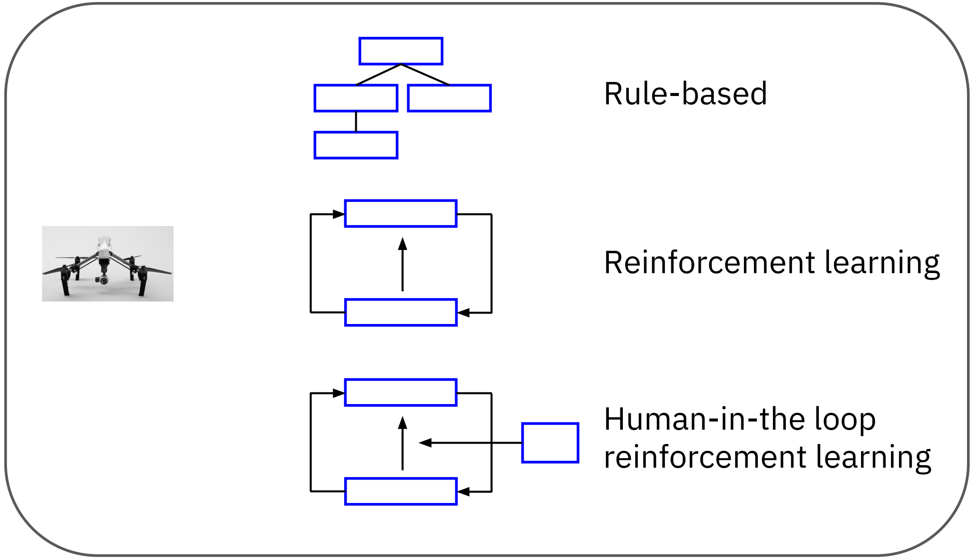
Horizontal Alternatives

> What system do we deploy?

Manned Unmanned Fully autonomous HMT

Vertical Alternatives

- How do we build the machine?



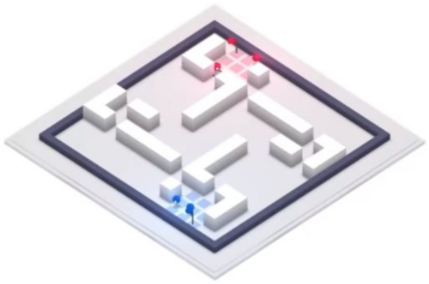
Rule-based Architecture

> **Design process**: Developer defines fixed rules of behavior for machine based on assumptions about the environment of deployment.

> **Execution**: Machine follows the rules based on a linear mapping of inputs to outputs.

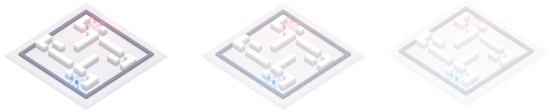
> **Limitations**: Machine depends completely on defined rules, cannot adapt.

> **Evaluation**: *Dependence on human input*: high, *generative behavior*: none, *execution capabilities*: high, *robustness*: low, *predictability*: high to medium.



Rule-based protocol:

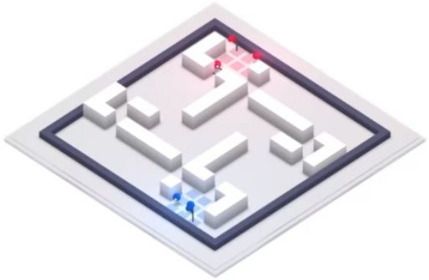
> move forward for n steps,
> turn left, move forward for k steps
> turn right, move forward for r steps
> turn left, move forward for e steps



Environment changes = substantial loss of performance

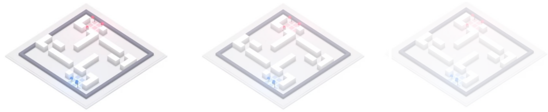
Reinforcement learning

- **Design process**: Developer specifies goal that she wants the machine to achieve and an algorithm that allows the machine to translate the goal into goal-achieving behavior, again based on assumptions about the environment of deployment.
- **Execution**: Machine evolves behavior to optimally reach the goal through elaborate trial-and-error process.
- **Limitations**: The developer has no control over what type of behavior the machine evolves.
- **Evaluation**: *Dependence on human input*: low, *generative behavior*: high, *execution capabilities*: high, *robustness*: medium, *predictability*: medium to low.



Reinforcement learning protocol:

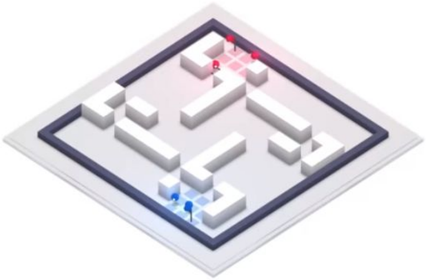
> reach red flag to receive high reward
> trial-and-error search process starts
> results in optimal way of behavior



Environment changes = limited loss of performance

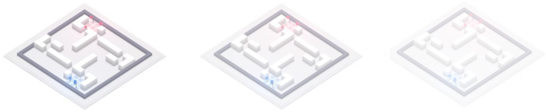
Human-in-the-Loop RL

- **Design process**: Same as for reinforcement learning, but a human can now intervene during the machine‘s learning stage by overwriting specific actions deemed undesirable.
- **Execution**: Machine again evolves behavior to optimally reach the goal through elaborate trial-and-error process, but a human can guide the machine‘s exploration.
- **Limitations**: The process of real-time human control of the machine‘s learning process is labor intensive.
- **Evaluation**: *Dependence on human input*: medium, *generative behavior*: medium, *execution capabilities*: high, *robustness*: high, *predictability*: high.



Human-in-the-loop RL protocol:

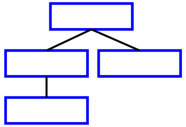
> reach red flag to receive high reward
> trial-and-error search process starts
> action *jump over wall* blocked by human
> results in optimal way of behavior



Environment changes = no loss of performance, if human remains in the loop

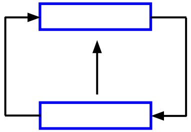
Summary of Vertical Alternatives

Rule-based



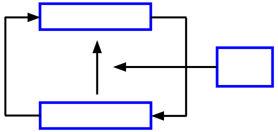
Give the system rules and it will adhere to them

Reinforcement learning



Give the system a goal and it will find a way to achieve it

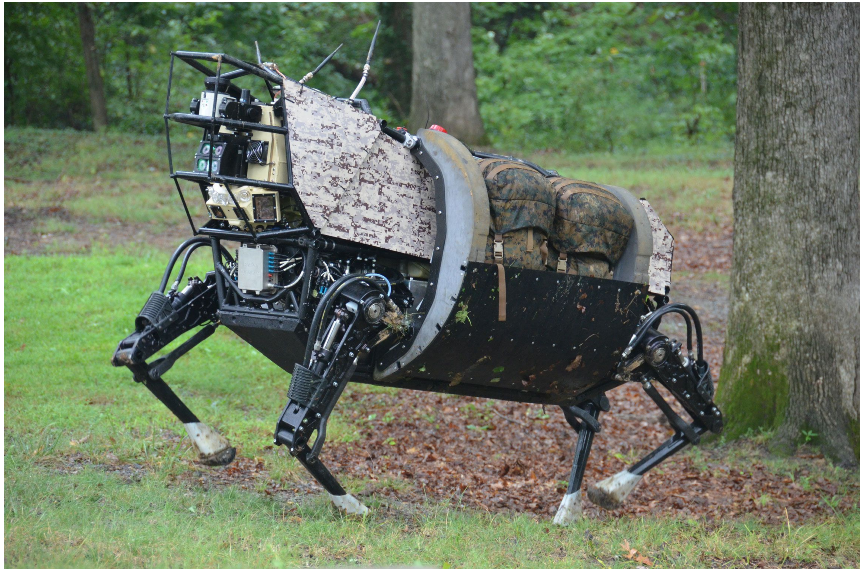
Human-in-the loop reinforcement learning



Give the system a goal and a supervisor and it will find a way to achieve the goal it a manner that aligns with the preferences of the supervisor

Logistics

- Safety and predictability most important
- Speed less critical due to expanded timescale
- Optimum level of automation depends on proximity to the battlefield, context - need for multiple modes

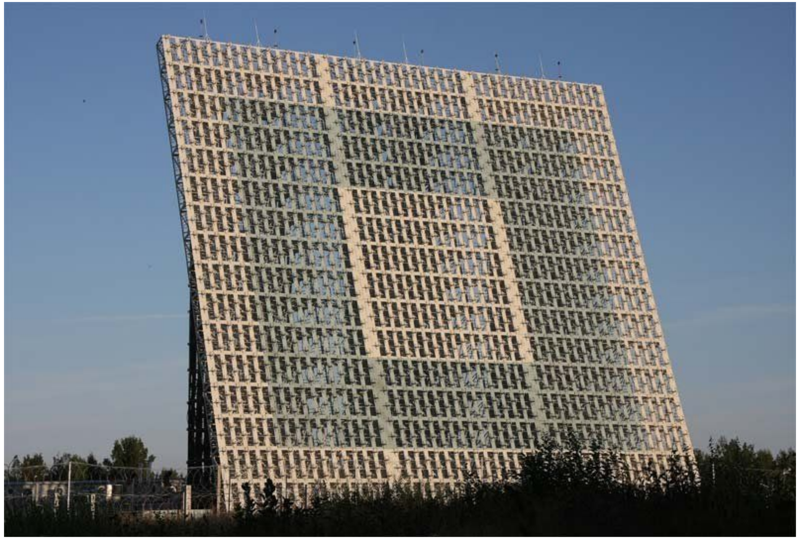


Logistics Concepts of Operations

- Adaptive logistics provision
  - Ensuring that resupply is efficient during periods of tactical surprise
- Semi-autonomous convoys
  - Lowering the number of people at risk
- Reduced manning for cargo aircraft
  - Saving pilots for other positions to make up for shortages

ISR

- Must be “auditable” to understand why it behaves a certain way
- Accuracy can be corrected by trained operators
- Optimum level of automation depends on speed of application and mission importance



ISR Concepts of Operations

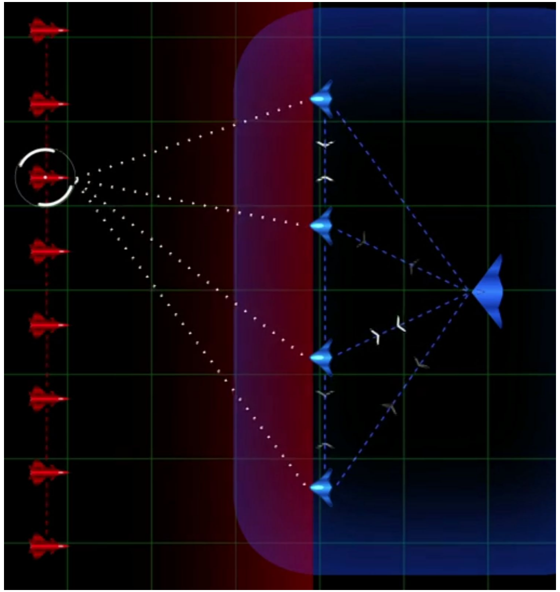
- Persistent swarm ISR for supporting ground operations
- Penetrating drones for sending back information via datalink from above A2AD Zones

Strike

- Ethics derives from safety and predictability
- Speed may not be as important as we thought
- Humans currently required to exercise “appropriate level of human judgment” per DOD Directive 3000.09

Strike Concepts of Operations

- IR drone teams or swarms with human target labelers
    - Enemy, civilian, friendly, and uncertain markers can be placed allow drones to efficiently attack following the laws of armed conflict, while helping the labellers avoid collateral damage
- Networked picket drones for protecting manned aircraft



Strategic Considerations

> National Innovation Capacity

- New model of government and industry collaboration and fusion

> Adoption Capacity

- Military
  - Bureaucratic inertia and organizational culture
  - Aligning new HMT operational concepts with existing human ones
  - Where does HMT fit? Willingness to cede control?
- If overcome:
  - Instant training & “ready-made” veterans
  - Does not require time for trust and integration into chain of command
- Political and Ethical Considerations

Strategic Considerations

> Extended Duration of Conflict

- Dangerous, dull, ”dirty” tasks left to machines
- Operator fatigue
- Minimize loss of life and human suffering through improved target discrimination, risk analysis, direct human engagement, and collateral damage mitigation
- Cost-effective

> Accelerated Pace of Conflict

- Compressed engagement timelines from missiles and short-warning saturation attacks
- Near instantaneous assembly and configuration into new fighting formation

> New Actors

- Lower barriers for entry and diffusion of capabilities for violence
- Enhanced end strength through “small, smart, many” strategy

Geopolitical Considerations

> Geo-space and Space + Cyberspace

- Changing security models and economic growth model:
  Technological trajectory determined by digital, data, and AI infrastructure

> Autocratic Regimes v. Democracies

- Top-down “civil-military fusion” and rapid adoption
- State-sponsored innovation & IP theft

> Weapon of the Weak or Powerful?

- Great Power Conflict: inequality of technological capabilities
- Asymmetrical Warfare