AI-enabled Real-time Situational Understanding at the Tactical Edge

ARO Adversarial ML Workshop
14 September 2017

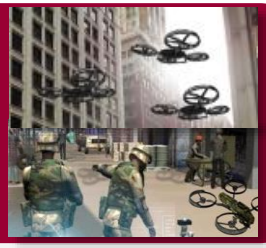
Tien Pham, PhD
Senior Campaign Scientist
Information Sciences Campaign

Topics

- Background: AI & ML Essential Research Area (ERA)
- AI-enabled Situational Understanding
- Collaborative Research Programs & Facilities with AI & ML

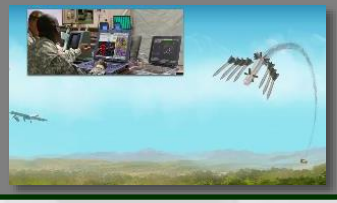
Essential Research Areas (ERAs)

Human-Agent Teaming

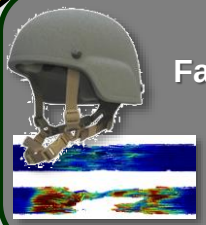


Cyber & EM Technologies for Complex Environments

Distributed / Cooperative Engagement in Contested Environments



Artificial Intelligence/ Machine Learning



Manipulate Failure Physics for Robust Materials

Tactical Unit Energy Independence

Manufacturing at the Point of Need

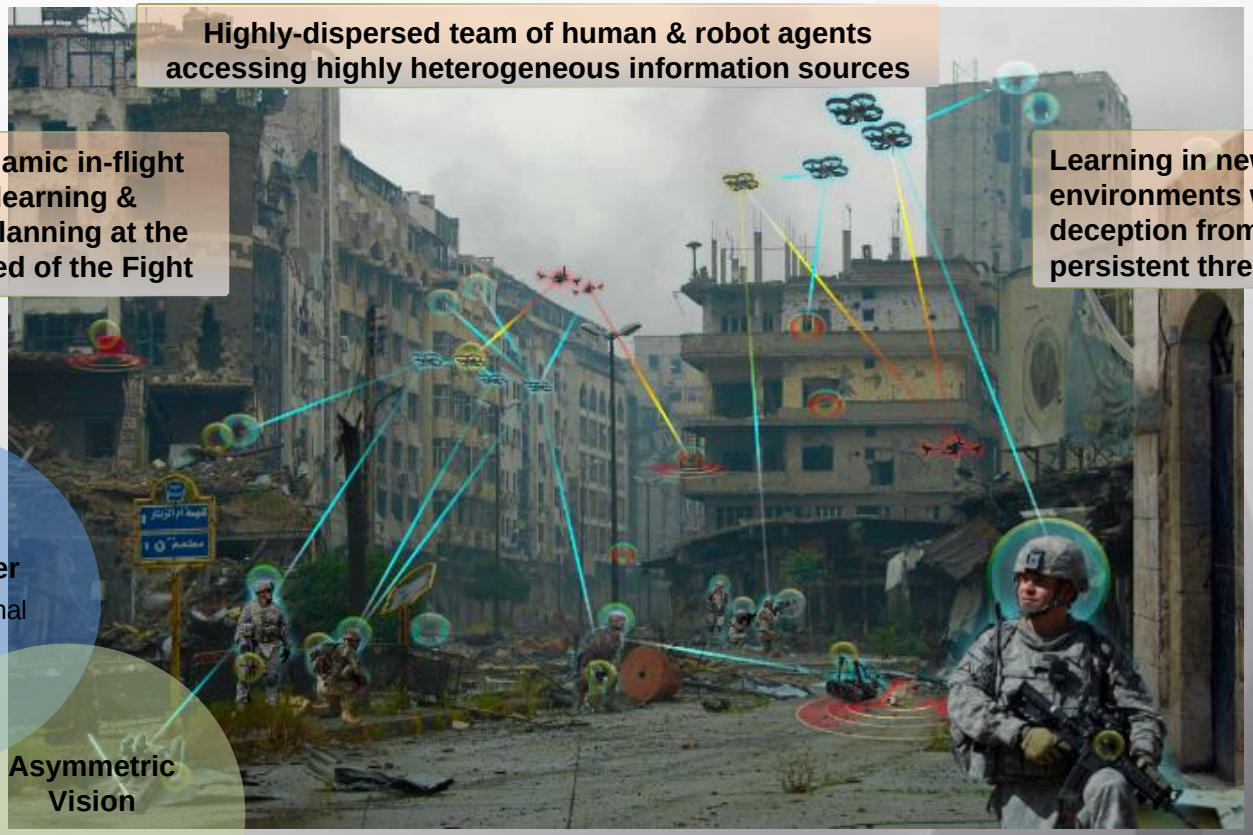
Accelerated Learning for a Ready Force

Discovery

The Nation's Premier Laboratory for Land Forces

Unified Land Operations → Prevailing in a Complex World

Large-scale, cluttered, contested urban environment



Highly-dispersed team of human & robot agents accessing highly heterogeneous information sources

Dynamic in-flight learning & re-planning at the Speed of the Fight

Learning in new environments with deception from persistent threats

Decide Faster
High Operational Tempo

Manned-Unmanned Teaming
Enhanced Mobility

Asymmetric Vision
Improved Situational Understanding

AI & ML Research Challenges

AI & ML Research Gaps

Learning in Complex Data Environments	→ AI & ML with small samples, dirty data, high clutter → AI & ML with highly heterogeneous data → Adversarial AI & ML in contested, deceptive environment
Resource-constrained AI Processing at the Point-of-Need	→ Distributed AI & ML with limited communications → AI & ML computing with extremely low size, weight, and power, time available (SWaPT)
Generalizable & Predictable AI	→ Explainability & programmability for AI & ML → AI & ML with integrated quantitative models

Goal: **To research and develop artificially intelligent agents (heterogeneous & distributed) that rapidly learn, adapt, reason & act in contested, austere & congested environments**

Potential Future Capabilities Envisioned

Combat Capabilities

→ Precision Engagement
→ Non-kinetic Engagement
→ Squad Sensors
→ Squad Autonomy

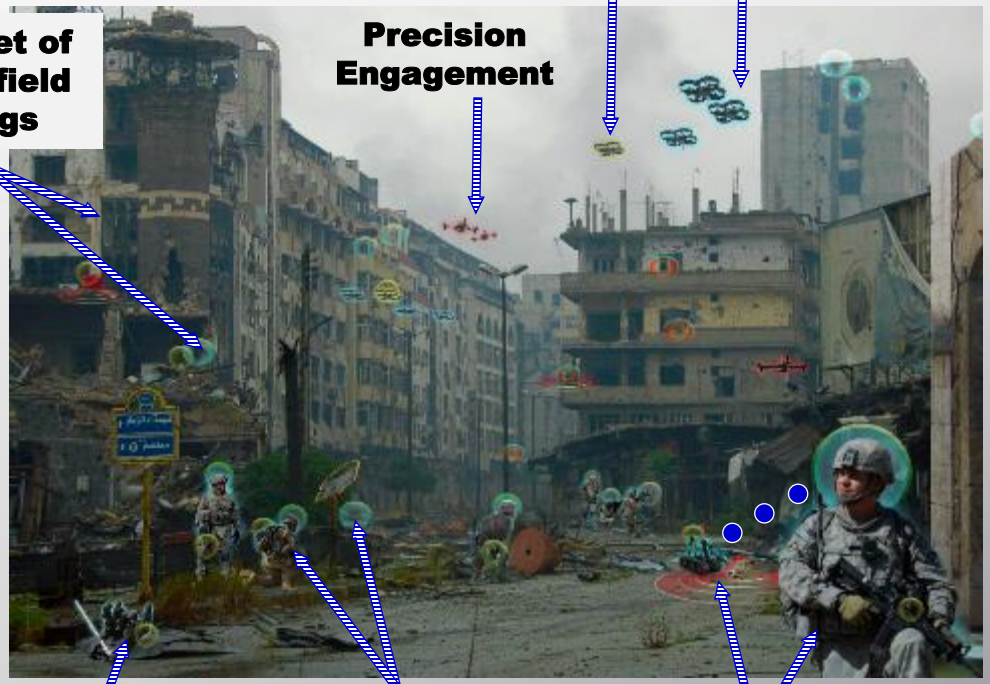
Autonomous UAV Swarms
→ ISR, force protection, BDA, network healing

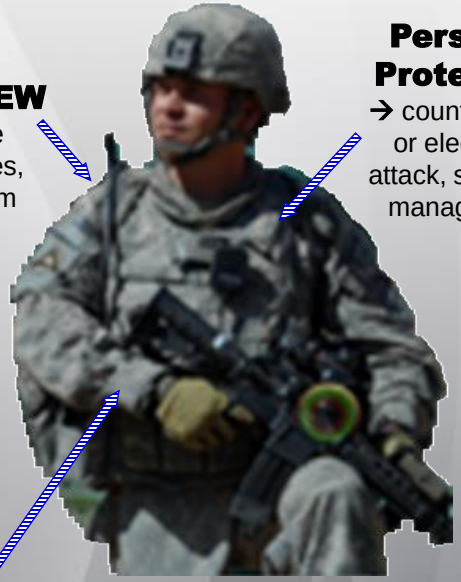
Cognitive EW & SIGINT

Augmented Reality for Multi-faceted Picture →
operational environment, friend-foe locations, activities, threats

Internet of Battlefield Things

Precision Engagement





SIGINT/EW
→ sense adversaries, evade, jam

Personal Protection
→ counter cyber or electronic attack, signature management

Wearable Electronics
→ biosensors, threat locators, sensors

Human-Machine Collaboration for Enhanced Decision Making

Net-enabled Semi-autonomous Weapons

Cognitive Networks
→ Network that perceives conditions, maintains memory, & adapts

Human-Robot Combat Teaming
(e.g., Man Un-Manned Teaming)

Topics

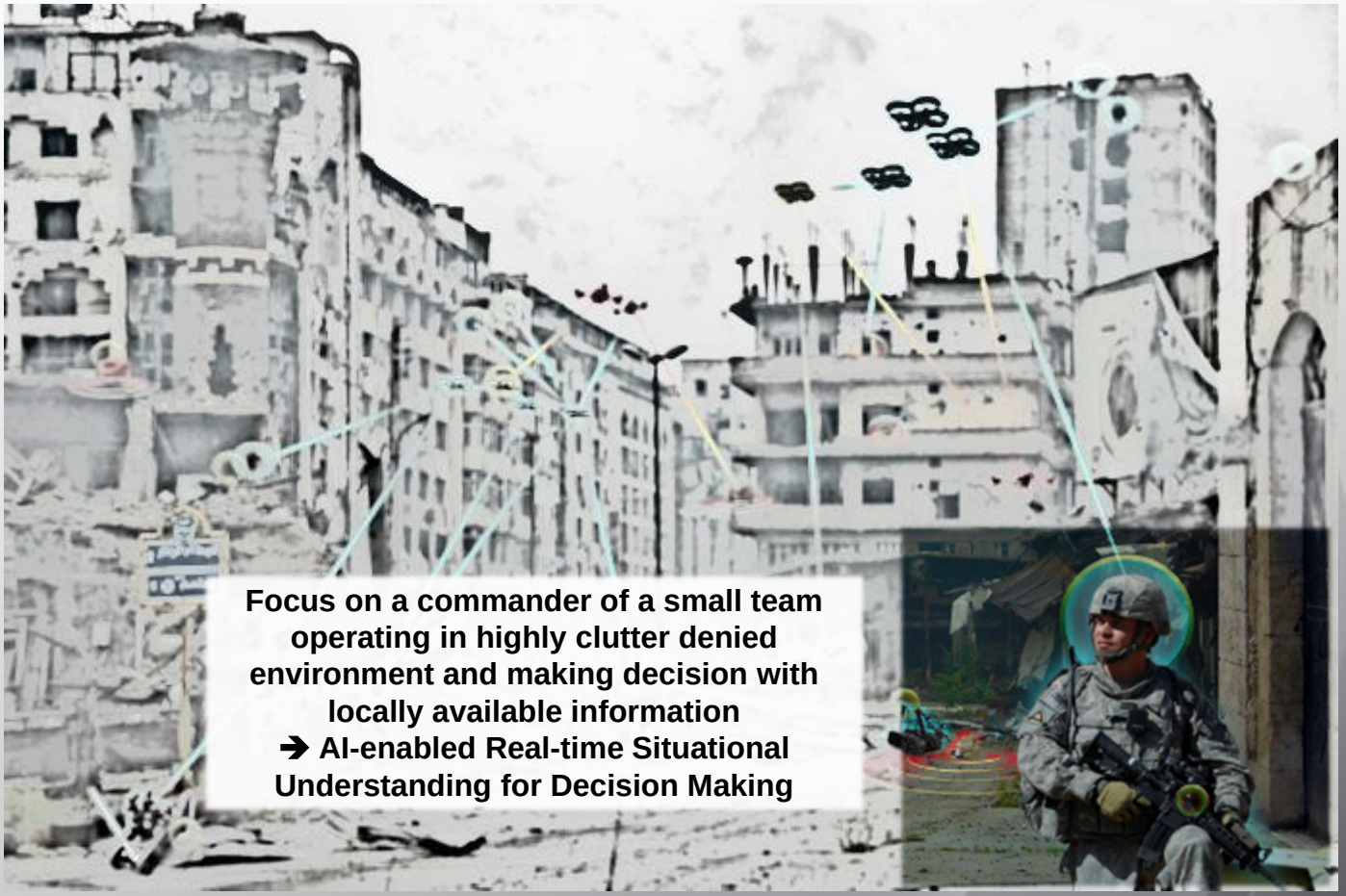
- Background: AI & ML Essential Research Area (ERA)
- **AI-enabled Situational Understanding**
- Collaborative Research Programs & Facilities with AI & ML

Unified Land Operations → Prevailing in a Complex World

Large-scale, cluttered, contested urban environment

Unified Land Operations → Prevailing in a Complex World

Large-scale, cluttered, contested urban environment



AI-enabled Real-Time Situational Understanding

Capabilities Focus: Enemy Estimates (SA) for Mission Command at the Edge in a distributed, complex, denied environment, with local resources

AI & ML ERA Focus: Learning and Reasoning in Complex Data Environments & Resource-constrained AI Processing at the Point-of-Need

AI & ML ERA

Adaptive Learning & Reasoning

→ AI that integrates adaptive learning inputs to generate tactically sensible enemy estimates at the Edge

→ Contribute to real-time decision-making in adversarial, cluttered, distributed environments

AI & ML Focused Efforts

1. Adversarial distributed ML
2. Robust inference & ML with conflicting sources
3. Adaptive online learning in real time
4. Adversarial reasoning integrating learned information
5. Resource-constrained adaptive computing for AI & ML

Conceptual Roadmap

Cumulative-Connected-Converged

(1) Adversarial Distributed ML

ML that is Robust and Resistant to Deceptive and Conflicting Inputs

(2) Robust Inference & ML

Reasoning about Enemy that Incorporates Distributed Learning

(4) Adversarial reasoning integrating learned information

AI for Generating Tactically-Sensible Estimates for Decision Making at the Edge

→ Distributed, Adversarially-robust, Resource-adaptive

(3) Adaptive Online Learning in real time

Adaptive Real-time Learning with Constrained Resources

(5) Resource-constrained adaptive computing

AI-enable Capability Scenario

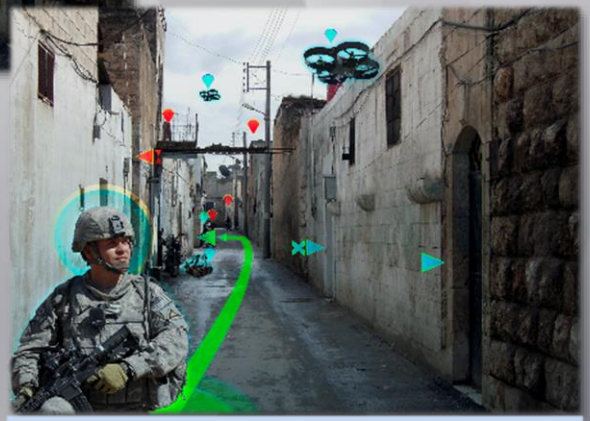
“Fight’s Eyes”

A Soldier supported by team of agents in complex environment

AI-enabled real-time estimates of enemy

AI-enabled reasoning to provide possible course of actions

Tactically sensible decision making based on locally available information



Focused Effort #1: Adversarial Distributed ML

Adversarial distributed ML robust to attacks in the face of peer adversaries

Vision: Theoretically-grounded approaches to distributed learning, particularly about the adversary, in a contested environment that is robust to deceptive inputs and that achieves quantifiably close-to-optimal performance under tactical network constraints. Enabling efficient learning with quantified uncertainty for situational understanding at the edge.

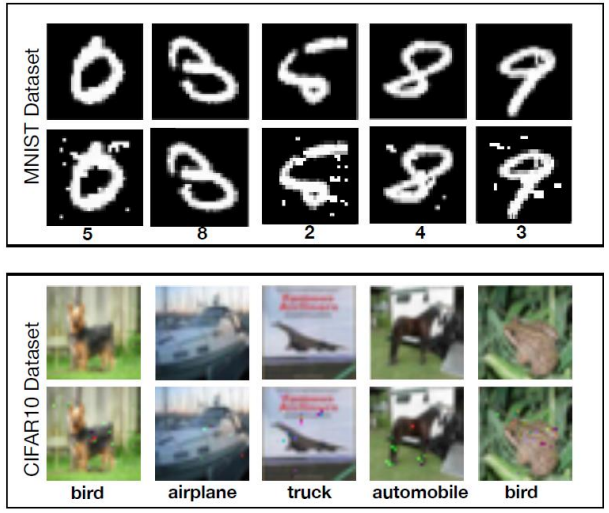


Figure taken from Papernot et al, IEEE S&P (Oakland), 2016

Research challenges & knowledge gaps:

- Characterization of intrinsic vulnerabilities arising from assumptions made in the modeling process
- Abstract realistic models of the attack surface of ML algorithms in training, inference, learning and adaptation
- Quantification of tradeoff between complexity of ML algorithms, accuracy, and resilience to adversarial manipulation
- Analytical understanding of the efficiency of an algorithm in an adversarial environment
- Development of near-optimal algorithms that provide quantifiable complexity-accuracy-resilience trade space

Why ARL?:

- Adversarial environment in literature has largely been benign (random noise and; anti-spam / anti-phishing efforts) with little effort except ARL Cyber CRA on modeling the intrinsic vulnerabilities of ML
- Unique Army challenges: dynamic at the edge operations, where data, context, processing, analytics, and situational understanding must be accomplished in distributed & dynamic environments and support collaborative decision making & mission command.
- Little research on ML with intermittent connectivity and tactical network constraints

Focused Effort #2: Robust Inference & ML

Robust inferencing & ML over heterogeneous, uncertain, and conflicting information

Vision: Characterize the fundamental limits of certainty that can be achieved for the mission variables with the (small) volume and (questionable) veracity of heterogeneous data various known/unknown sources. Develop inference algorithms that achieve or come close to optimal.

Research challenges & knowledge gaps:

- Salient representations of heterogeneous data (representing both sensor and human generated feeds) for semantic capture of the mission learned over sparse samples
- Detection of conflicting data in light of its advertised uncertainty
- Characterize behavior of sources based on their conflict history
- Fusion at the tactical edge in a manner that accurately represents uncertain knowledge of the ground truth to support decision making.
- Uncertain probabilistic models that capture the precision of knowledge gleaned from sparse data

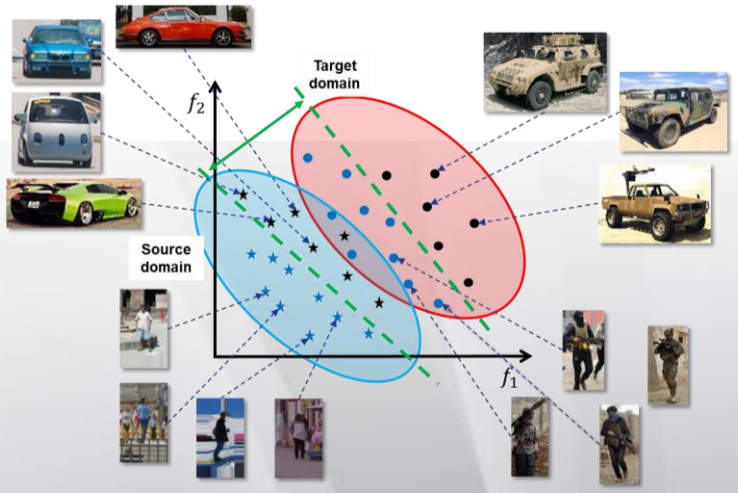
Why ARL?:

- Research community is focused on developing learning approaches to enable robust inferences for problems where large datasets and computational resources are available.
- There has been little effort (apart from ARL-funded collaborative efforts) that addresses processing at the edge with sparse training data and limited opportunities to share relevant data across teams that will lower uncertainty and give mission command the information they need.

Focused Effort #3: Adaptive Online Learning

Adaptive online learning for dynamic environmental changes in real time

Vision: Theoretically-grounded approaches for adaptive online learning that can acclimate using very few data samples. Enable modeling limited, dirty data in real-time that can: (i) continue to extract environment information from data sources despite differences between training and deployment and dynamic changes in battlefield conditions, and (ii) be dynamically reconfigured to recognize new classes of objects.



Research challenges & knowledge gaps:

- Development of non-traditional machine learning approaches and techniques that (i) do not require vast amount of training data and (ii) can learn as data becomes available (unlike traditional DNN's)
- Quantification of the trade space for accuracy: fundamental understanding of how mission context, global consistency modeling, and reasoning interact with and drive the requirements for accuracy
- Fundamental understanding of open set recognition for perception systems that seek to grow their capabilities
- Opportunistic domain adaptation that can recognize and correct for shifting data distributions with both unsupervised or labeled, potentially multi-modal, data

Why ARL?:

- Future Army systems must deal with dynamic battlefield environments that are unknown a priori and that feature extreme clutter and high-consequence training mismatch which is a unique Army problem.
- Adaptive learning (for navigation) is being studied under collaborative research effort such as the MAST and Robotics CTAs and will be studied under the upcoming DCIST CRA. The groundwork for this effort has been done by ARL researchers studying online sparse non-parametric learning and unsupervised semantic scene segmentation.

Focused Effort #4: Adversarial Reasoning

Intelligent adversarial reasoning integrating learned information from disparate & distributed ML inputs

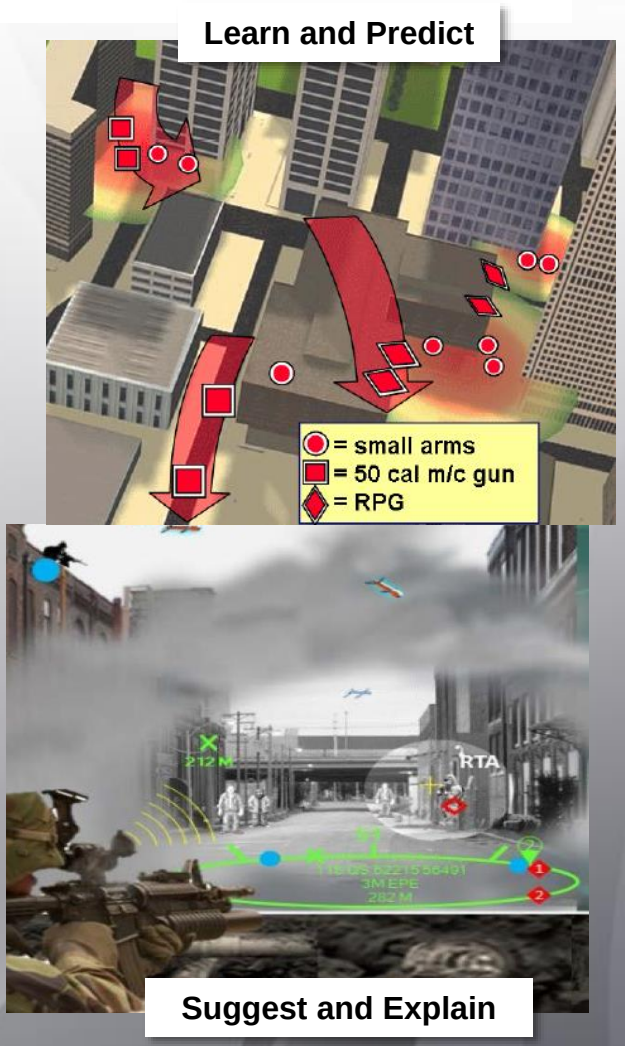
Vision: Theoretically-grounded approaches for generating enemy estimates (what the enemy is doing, and what it will do) based on continuous dynamic learning; mindful of enemy concealment and deception; explainable and insightful for the commander

Research challenges & knowledge gaps:

- Approaches to adversarial reasoning that leverage continuously learned, disparate knowledge sources
- Theoretically supported and learning-guided detection of probable enemy deceptions (incl. concealment)
- Methods to formulate explainable results that are insightful for human commanders' near-instant decisions
- Approaches for characterizing reliability of the computational reasoning's results
- Generalized models for continuously machine-learned knowledge aligned with adversarial reasoning

Why ARL?:

- Ground warfare presents diversity and uncertainty that far exceed current scope of industry/academia research in adversarial learning
- Research in industry/academia concentrate on resource-rich or closed domain problems; on adversarial learning but not adversarial reasoning



The Nation's Premier Laboratory for Land Forces

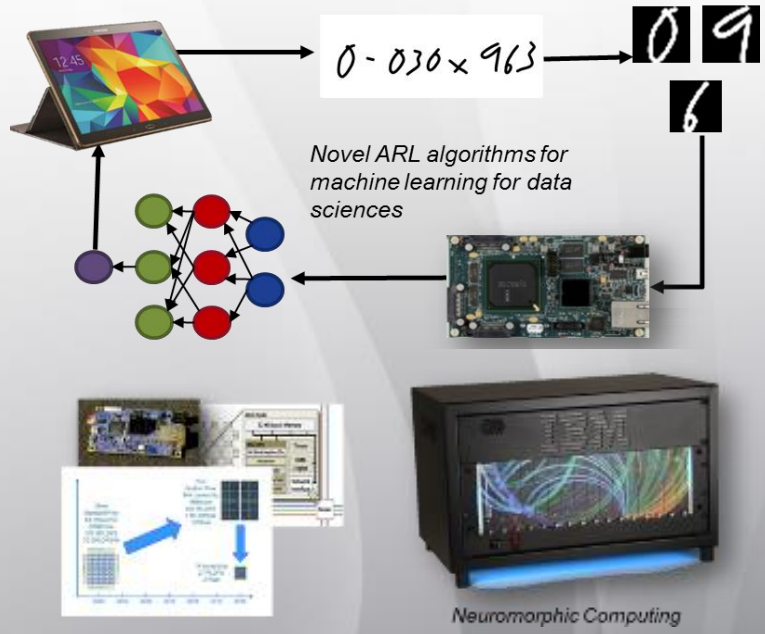
U.S. ARMY RDECOM

Focused Effort #5: Resource-constrained Adaptive Computing

ARL

Hardware & software for adaptive computing for SWAPT-constrained learning & reasoning

Vision: Novel heterogeneous computing resources, such as neuromorphic and other processors, dynamically allocated, adapted and accessed for demanding AI&ML processing. Algorithms and software dynamically adaptive for on-line learning and reasoning using extremely low SWAPT computing resources under constraints of limited communications.



Research challenges & knowledge gaps:

- Techniques for adaptive allocation of computing resources to tasks in an environment with rapidly changing connectivity and availability of assets
- Real-time adaptation of algorithms for available hardware, tasks and time available
- Methods for optimized real-time reconfiguration of hardware based on properties of the tasks and available software
- Characterization of capabilities and constraints of novel computing architectures (e.g., neuromorphic) for learning and reasoning processes
- Approaches to implementing AI&ML algorithms on non-von-Neumann architectures

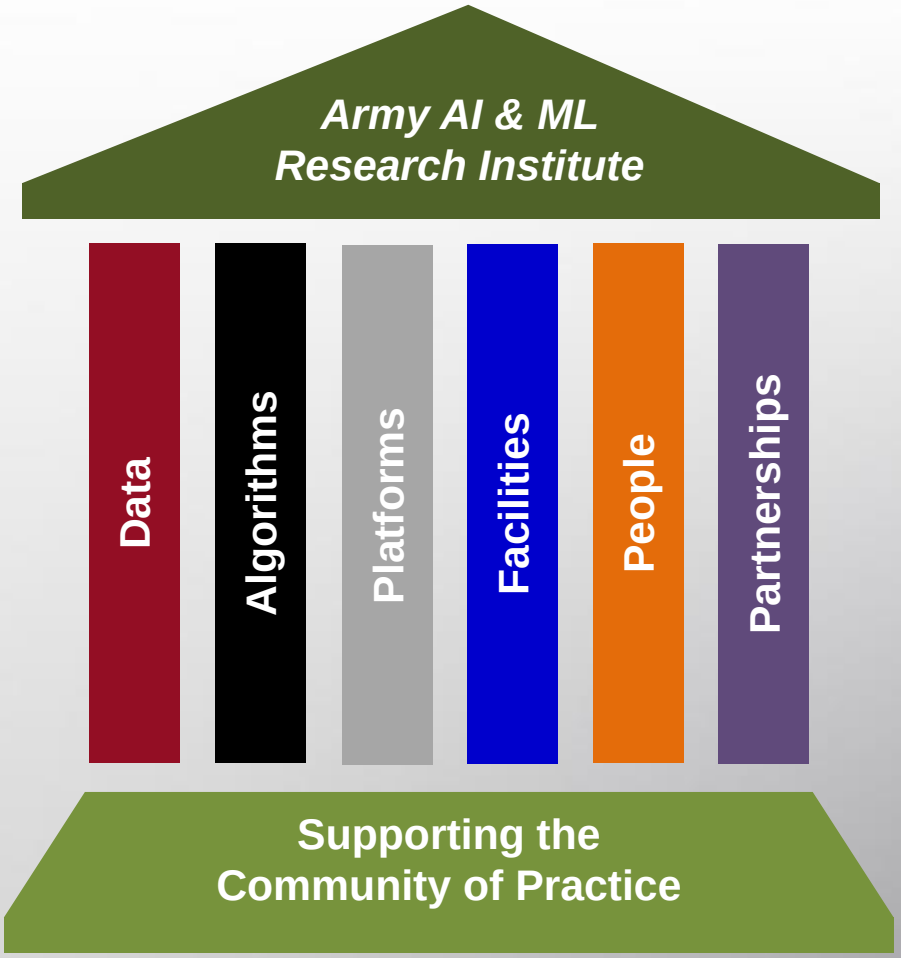
Why ARL?:

- Ground warfare in urban and similar environments will rely on distributed small platforms, with highly constrained SWAPT, in rapidly changing collaboration topology

Topics

- Background: AI & ML Essential Research Area (ERA)
- AI-enabled Situational Understanding
- **Collaborative Research Programs & Facilities with AI & ML**

Enabling Research Concept



Goals

- **To enable collaborative research to develop *Generalized AI* capabilities and *Robust AI* technologies for complex adversarial environments**
- **To serve as the focal point for Army research in AI & ML:**
  - Facilitate multi-disciplinary collaborative research with academia, industry and other government organizations
  - Establish accessible database of heterogeneous data, repository of AI & ML algorithms and software tools, military relevant use-cases and challenge problems, AI & ML experts & military SME's
  - Coordinate and sponsor joint experiments and demonstrations
  - Share state-of-the-art results and lessons learned

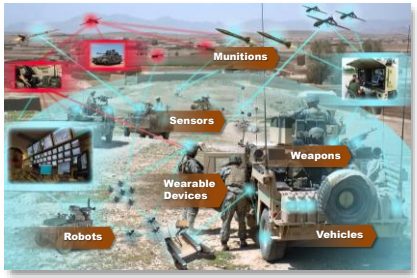
New Collaborative Programs & Facilities

Programs & Facilities: Enable collaborative, multi-disciplinary and cross-ERA research in Information Sciences

Distributed Analytics & Information Sciences ITA

Started in Sep 2016

Internet of Battlefield Things (IoBT) CRA



New Start in Oct 2017

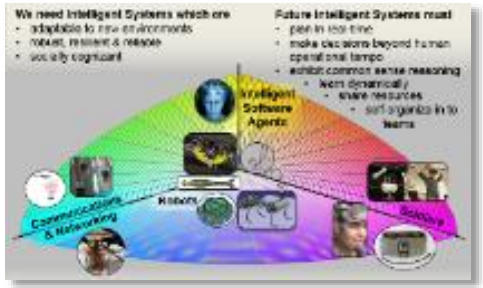
Distributed Collaborative Intelligent Systems (DCIST) CRA

New Start in Oct 2017

Network Science Research Lab (NSRL)

Opened in Apr 2016

Intelligent Systems Center (ISC)



Available in FY18

Sensor Information Testbed Collaborative Research Environment (SITCORE)

Available in FY18

The Nation's Premier Laboratory for Land Forces

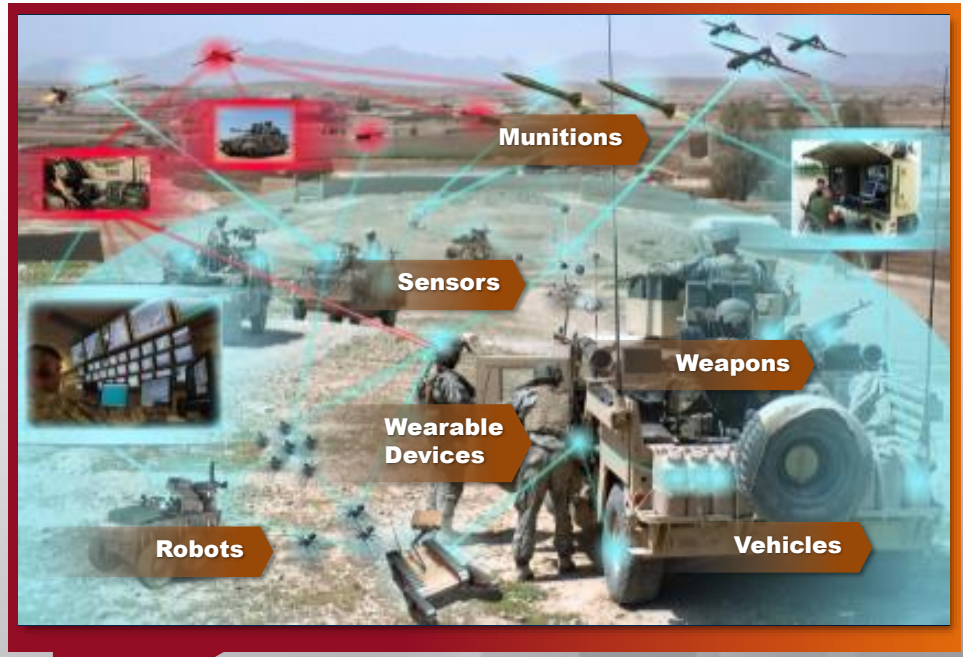
BACK UP

Internet of Battlefield Things (IoBT) CRA

Supporting S&T Campaigns: Information Sciences, Computational Sciences and Human Sciences

An IoBT is a *set* of interdependent entities or things

- Sensors, actuators, devices (e.g.,computers, weapons, vehicles, robots, human-wearables)
- Infrastructure (networks, storage, processing)
- Analytics (on-node, in-network, centralized)
- Information Sources & Open Source Intelligence
- Humans



Research Areas

- RA1: Discovery, Composition and Adaptation of Goal-Driven Heterogeneous IoBTs
- RA2: Autonomic IoBTs to Enable Intelligent Services
- RA3: Distributed Asynchronous Processing and Analytics of Things
- CCRI: Cyber-Physical Security

Supporting S&T Campaigns: Science for Maneuver
Human Sciences and Information Sciences

DCIST Vision

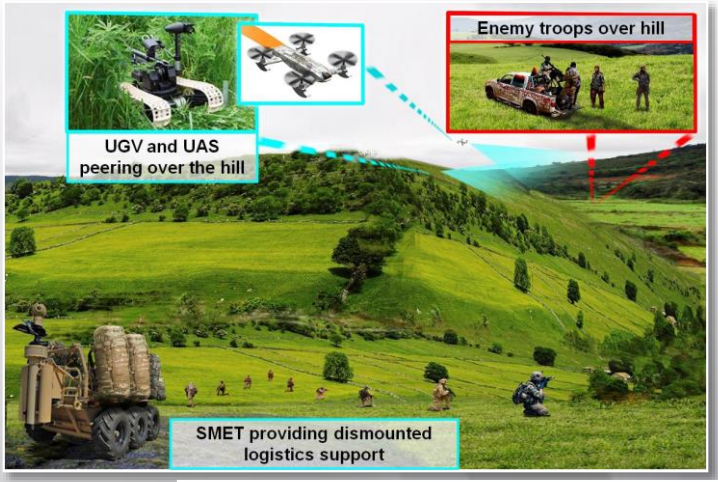
- Highly distributed and collaborative heterogeneous teams of intelligent systems
- Integrate varying levels of autonomy and intelligence with the Soldier
- Augment the capability of the collective well beyond that of any one component

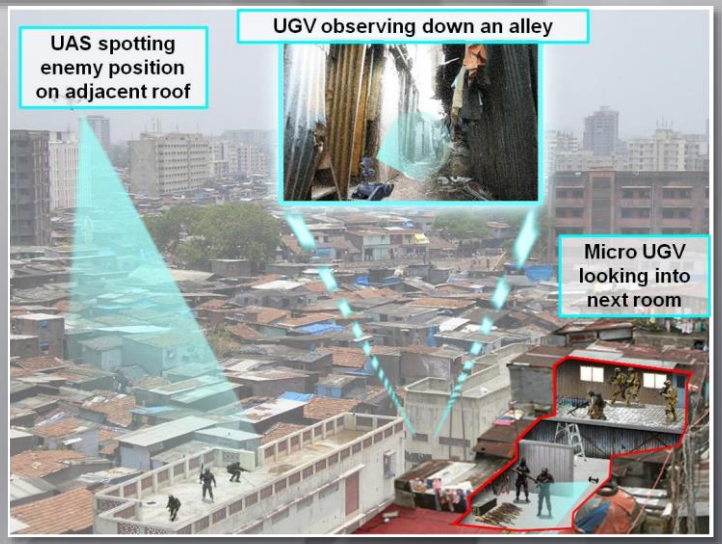
Payoff

- Extended reach, SA, and operational effectiveness against dynamic threats in contested environments
- Technical & operational superiority through intelligent, resilient & collaborative behaviors

Research Areas

- RA1: Distributed Intelligence
- RA2: Heterogeneous Group Control
- RA3: Adaptive and Resilient Behaviors





U.S. ARMY RDECOM®

NSRL - Open Campus Facility

ARL

Network Science Research Laboratory (NSRL) opened in Apr 2016

Goal:

Research, infrastructure, software support tools, and expertise to support:

- **Foundational research** on the complex interactions of heterogeneous networks
- **Collaboration** between government, academia, industry researchers regardless of nationality

Payoff:

- **Improved tactical communications**, sensing, command and control and **decision-making**
- More robust tools for network designers, military analysts & Soldiers

Purpose:

Create a ***collaborative*** experimentation workspace for solving ***complex trans-disciplinary problems***

Provide the infrastructure to experiment, prototype and demonstrate future capabilities of ARL's ***network science research*** program

https://www.youtube.com/watch?v=bv8XPn57sDI

The Nation's Premier Laboratory for Land Forces

Intelligent Systems Center (ISC)

BACKGROUND

On the future battlefield, intelligent robots will be ubiquitous Soldier teammates. Future Intelligent Systems must conduct operations in challenging, militarily relevant environments, operate in concert with Soldiers and commanders, collaborate with other intelligent systems, and make decisions within and beyond human operational tempo. The ARL Intelligent Systems Center (ISC) will facilitate innovation by encouraging cross-disciplinary research with the focus on long-term basic and applied research. The Center will leverage the strength of its current research program by focusing on systems that interact with the physical world.

COLLABORATIVE FOCUS

Highly collaborative environment with cross-discipline opportunities in:

- Traditional Robotics (Intelligence, Perception, and Mobility/Manipulation)
- Adaptive Control
- Autonomous Networking
- Distributed Computing (HPC)
- Machine Learning & Artificial Intelligence
- Cognitive Architectures
- Natural Language
- Semantics
- Game Theory
- Reasoning, Knowledge Engineering
- Trust and Transparence
- Testing, Evaluation, Validation and Verification

BENEFITS

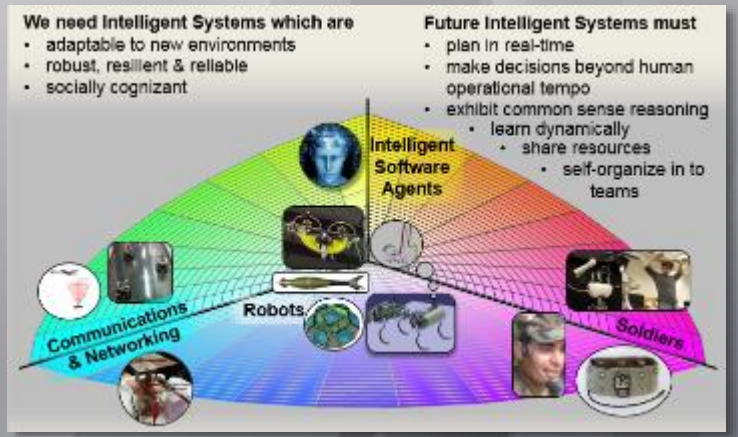
- Robotic Experimental Hardware (ground & air)
- Intelligent Algorithm Software Repository
- Unique Military Data Sets
- Simulation Tools

UNIQUE FACILITIES

- Emmerman Intelligent Systems Laboratory (Adelphi, MD)
- UAV Test Flight Facility (APG, MD)

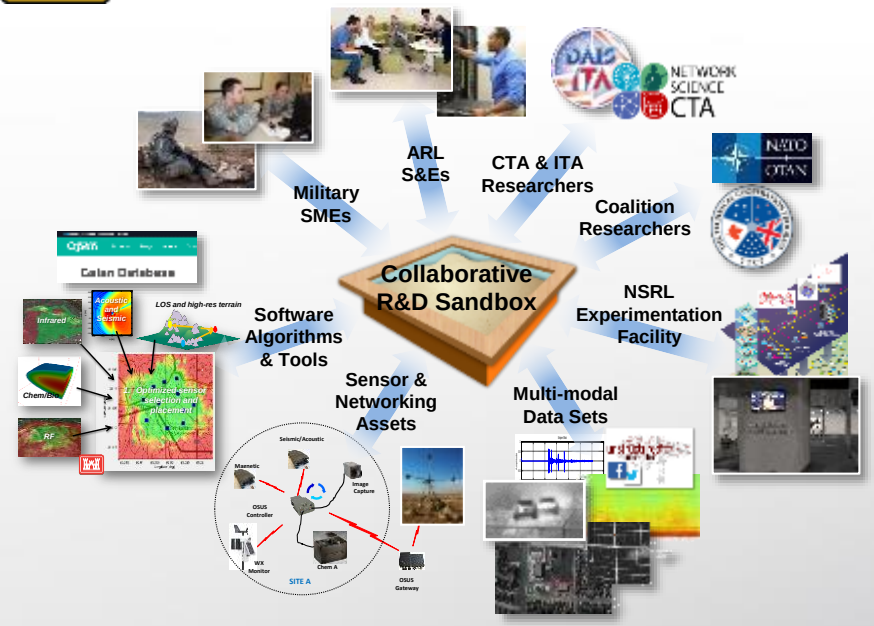
CONCEPT OF OPERATION

The ISC will utilize CRADAs, MOUs and/or MOAs to define the extent of collaboration under the center, the disposition of intellectual property, and the sharing of research outcomes and laboratory resources.



The Nation's Premier Laboratory for Land Forces

Sensor Information Testbed Collaborative Research Environment (SITCORE)



Collaborative Focus: Provide critical enablers for algorithm development including facilities, software tools, data, use cases and technical & operational subject matter experts

Highly collaborative R&D environment under Open Campus with focus on sensor data & information fusion leveraging the following:

- Guest researchers from universities, industry, and collaborative technology/research alliances
- Other Government agencies & coalition partners

Benefits: Provides physical space and collaborative software tools with access to:

- ARL researchers & Army operational experts
- Military-relevant data sets and database tools
- Specialized processing algorithms and toolboxes
- Specialized sensors and other ISR assets
- Potential end-users for technology transition
- Virtual research capability to allow collaboration from remote locations

Unique Facilities: Direct access & link to other ARL Open Campus facilities and external partners

- Network Sciences Research Laboratory (NSRL)
- Intelligent Systems Center (ISC)
- Automated Online Data Repository (AODR)
- Open Standard for Unattended Sensors (OSUS) System Integration Lab (SIL)
- Secure Unclassified Network (SUNet) enclave