

Session 13:  
Military Internet of Things (IoT), Autonomy,  
and Things to Come

**Niranjani Suri, Ph.D.**

US Army Research Laboratory, Adelphi, MD &  
Florida Institute for Human & Machine Cognition (IHMC), Pensacola, FL

**Mauro Tortonesi, Ph.D.**

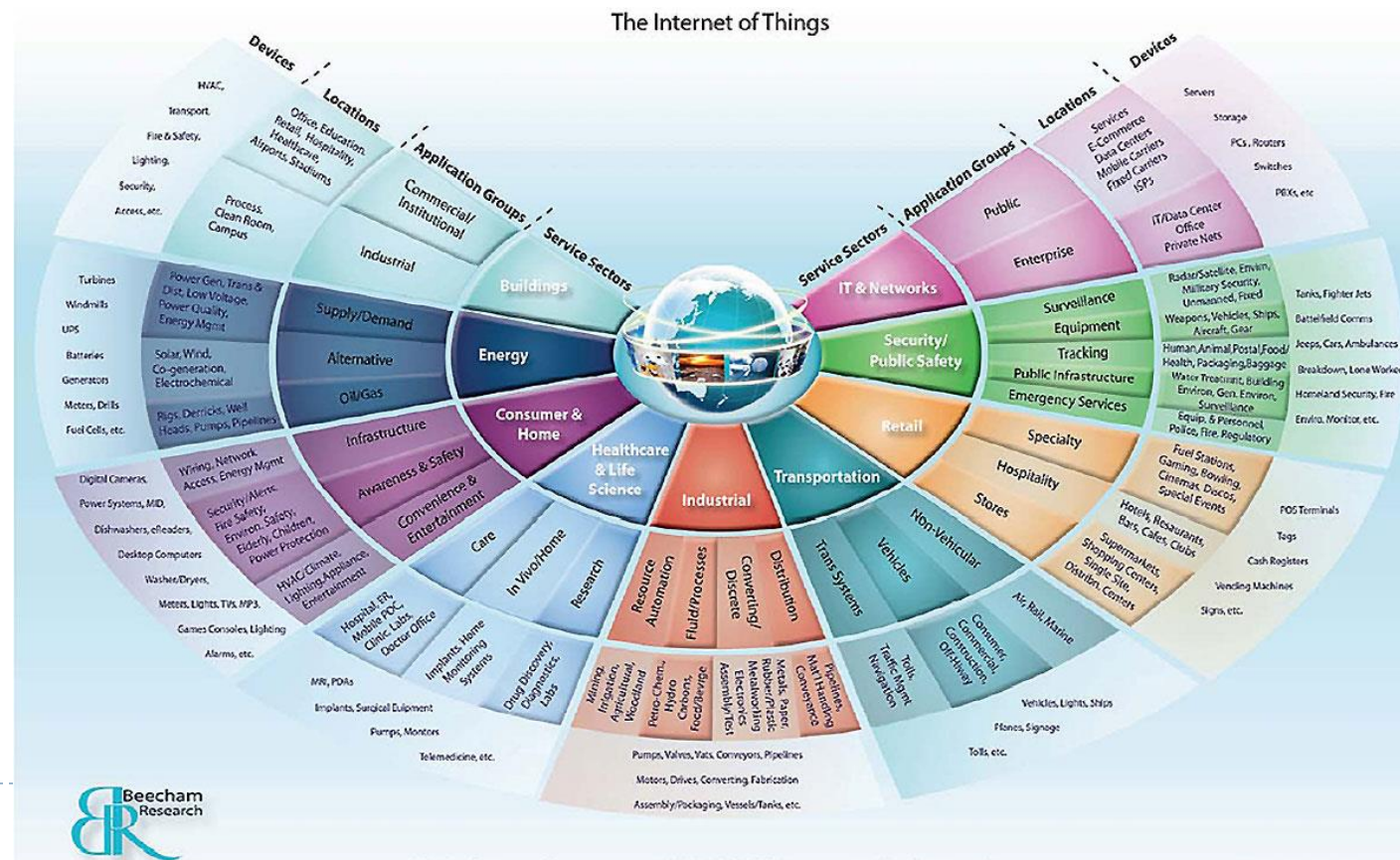
University of Ferrara, Italy

# Motivation

- Internet of Things will be (already is?) everywhere
- The military community cannot ignore ongoing developments in IoT
  - ▶ At a minimum, IoT will be forced on the Military by the commercial supply chain (e.g., RFID)

• If IoT will permeate our daily lives and environment, it will certainly affect, if not permeate, the military environment

- We must
  - Understand
  - Defend against
  - Leverage
  - Exploit



# Characteristics

---

The Internet of things is the realization of pervasive computing, communication, and sensing

- Everything will be a sensor, a processor, and a communicator (increased number of heterogeneous devices, connectivity, and communication)
  - Biosensors (e.g. pills/chemicals, plants, people, etc.)
  - Traditional sensors (e.g. environmental sensing devices , etc.)
  - Non-Traditional sensors (TV's, appliances, humidifiers, clothing, etc.)
- The “battle space” (operating space?) will consist of active red, blue, AND gray
  - Deception will be the norm
  - Environment will be dynamic (e.g. megacities and rural)
  - Ownership and other boundaries will be diverse and transient
- Increased complexity for the Warfighter
  - Situation-adaptive responses
  - Real time sense making over massive heterogeneous data
  - Selective collection and processing



# Requirements for Military Use

---

- **Decentralized Infrastructures**
  - Cannot rely on centralized clouds
  - Tactical clouds – still questionable (data still distributed)
- **Network Utilization**
  - Not a challenge for most commercial environments
  - Single hop connectivity to the Internet
- **Interoperability**
  - Some standard protocols exist, but typically involve licensing
- **Trust and Security**
  - Privacy is the primary concern, but manufacturers want complete access
- **Sensor and Device Utilization**
  - Power is still a challenge
- **Applications of Semantic Web Technologies**
  - Could help with interoperability, data analysis, exploitation



# The Autonomy Connection...

---

- ▶ **Autonomy has been identified as a major requirement by the US DoD**
  - ▶ US Army Third Offset Strategy to address A2AD challenges
  - ▶ OSD Autonomy Research Pilot Initiative (ARPI)
  - ▶ DoD Defense Science Board Study on Autonomy
    - ▶ Report: The Role of Autonomy in DoD Systems (July 2012)
    - ▶ Report: Summer Study on Autonomy (June 2016)
- ▶ **Autonomy promises to address many challenges:**
  - ▶ Anti-access / Area-denied (A2AD) situations
    - ▶ Disrupted communications
  - ▶ Rapid reaction time
- ▶ **But also raises many challenges:**
  - ▶ Human-in-the-loop moving to Human-on-the-loop
  - ▶ Opaqueness of decision making
- ▶ **Autonomy, Self Organization, Self Adaptation are likely key to managing IoT and the associated growth in devices and information**



# Questions for the Panelists

---

- ▶ What are potential military applications of IoT concepts?
- ▶ What are the new C2 challenges that arise from IoT? Solutions?
- ▶ What aspects of commercial IoT can be leveraged in the military context?
- ▶ What are unique challenges in the military environment?
- ▶ What are some envisioned roles for autonomy in the DoD problem space?
- ▶ What are some anticipated future problem spaces that also demand autonomy and intelligent systems?
- ▶ How can trust be addressed to improve confidence in autonomy?
- ▶ How can humans and autonomous systems collaborate?
  
- ▶ Is IoT creating a new problem? Or more of the same?
- ▶ Are we already behind the curve?



# Panelists

---

- ▶ Lt. Col. Adrian Woodley (UK Army HQ)
- ▶ Dr. James Michaelis (Army Research Laboratory, USA)
- ▶ Dr. Michael Gerz (Fraunhofer FKIE, Germany)
- ▶ Mr. Thomas Remmersmann (Fraunhofer FKIE, Germany)
- ▶ Dr. Michael Hieb (George Mason University, USA)





# Military Internet of Things

Lt Col Adrian Woodley

Army HQ





# A View from the Ground

- Military Applications
- C2 challenges
- Environmental Constraints



# Military Applications

- Human Performance tracking
- Medical tracking
- Logistic tracking
- Unmanned Systems
- Every platform a sensor



# C2 Challenges

Driven by Environmental Constraints



# Our Office





# C2 Challenges driven by Environmental Constraints

- Internet Characteristics
  - High capacity static backbone
  - Wireless connectivity
  - Limitless storage
- Military networks
  - If we want it, we have to take it with us
  - Significant time to build and manage



# C2 Challenges driven by Environmental Constraints

- Security
  - Physical
  - Electronic
- Spectrum
- Big Data



## **Session 13: Military Internet of Things (IoT), Autonomy, and Things to Come**

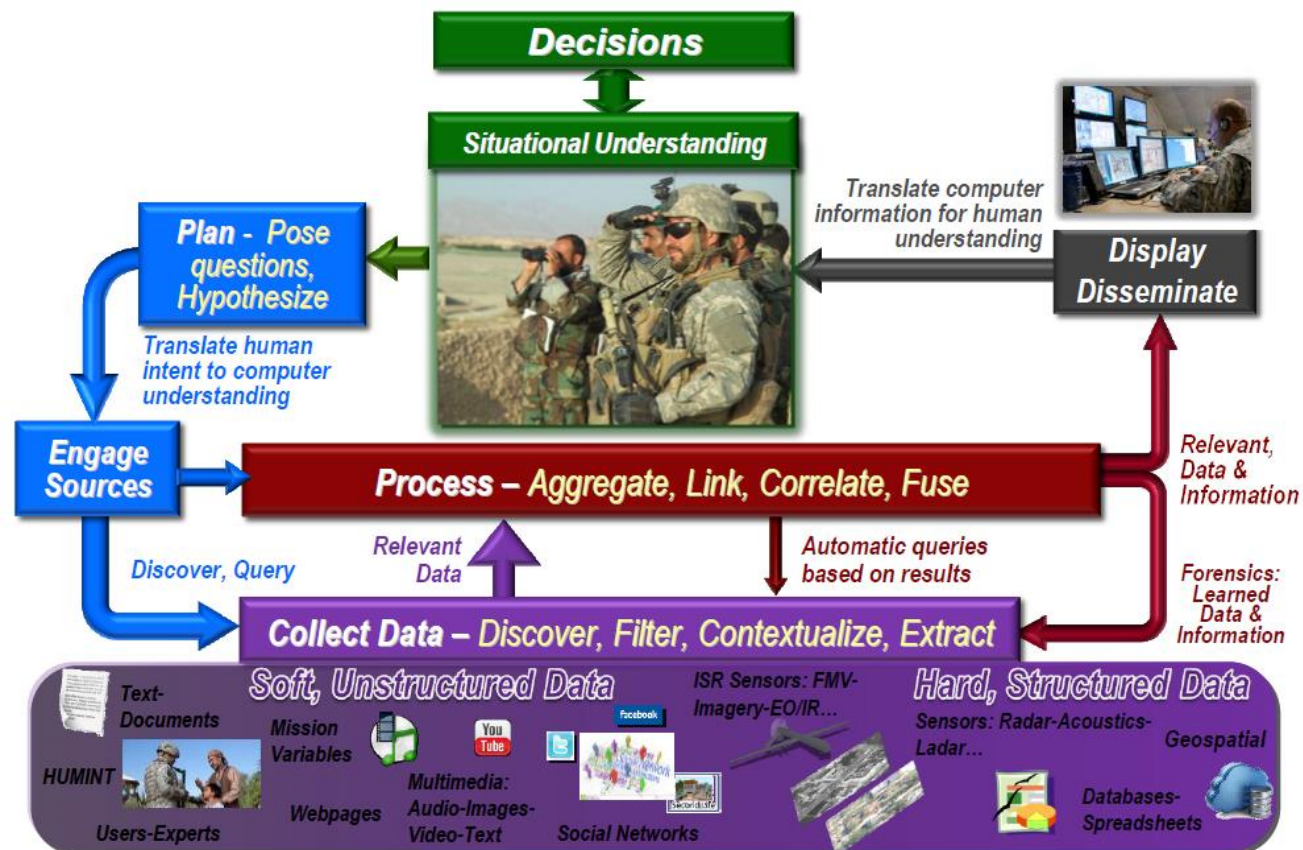
*21st International Command and Control Research and Technology Symposium (ICCRTS)*

*September 6-8, 2016*

**James R. Michaelis**

**U.S. Army Research Laboratory, Adelphi, MD**

The Internet of Things (IoT) stands to provide new means for establishing C2 situational understanding



IoT technologies offer promise for data gathering, as well as information generation and dissemination

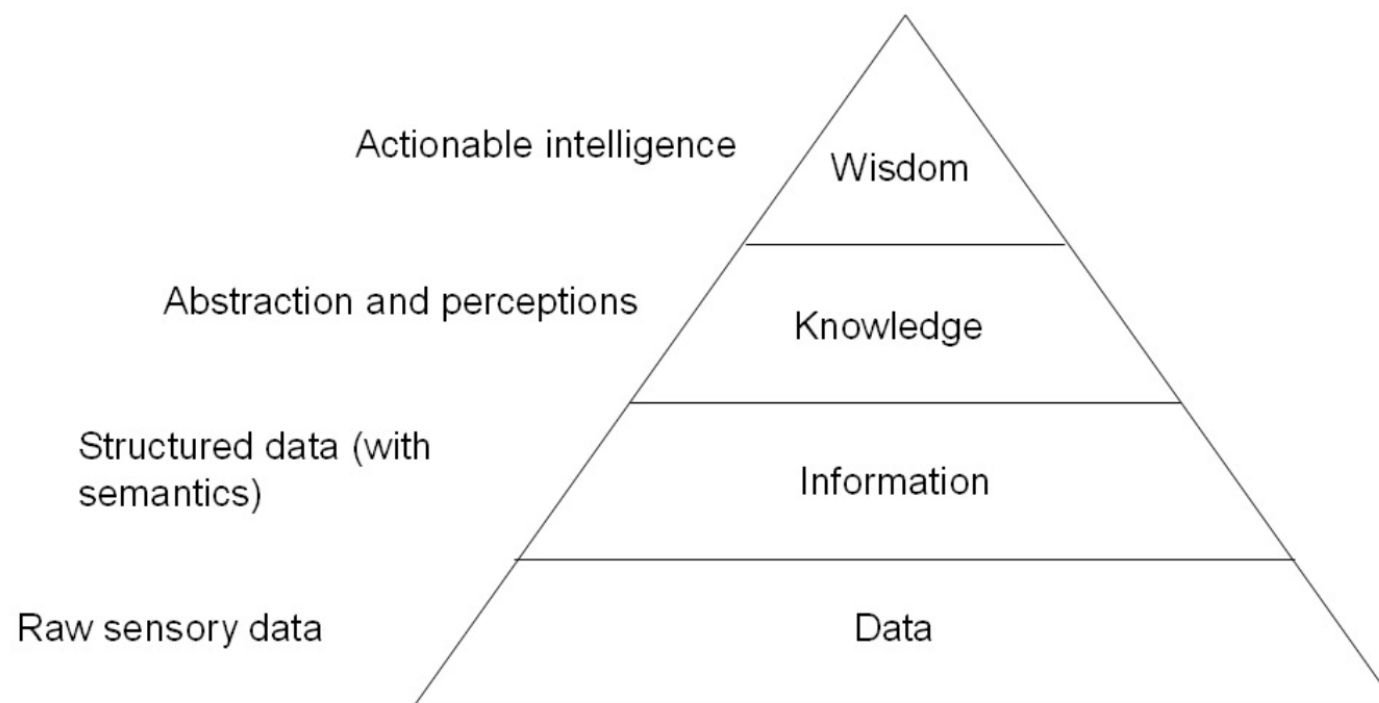




# Information Actionability within IoT



Actionable intelligence from IoT sources hinges upon access to meaningfully structured information collections [Barnaghi, 2012]:



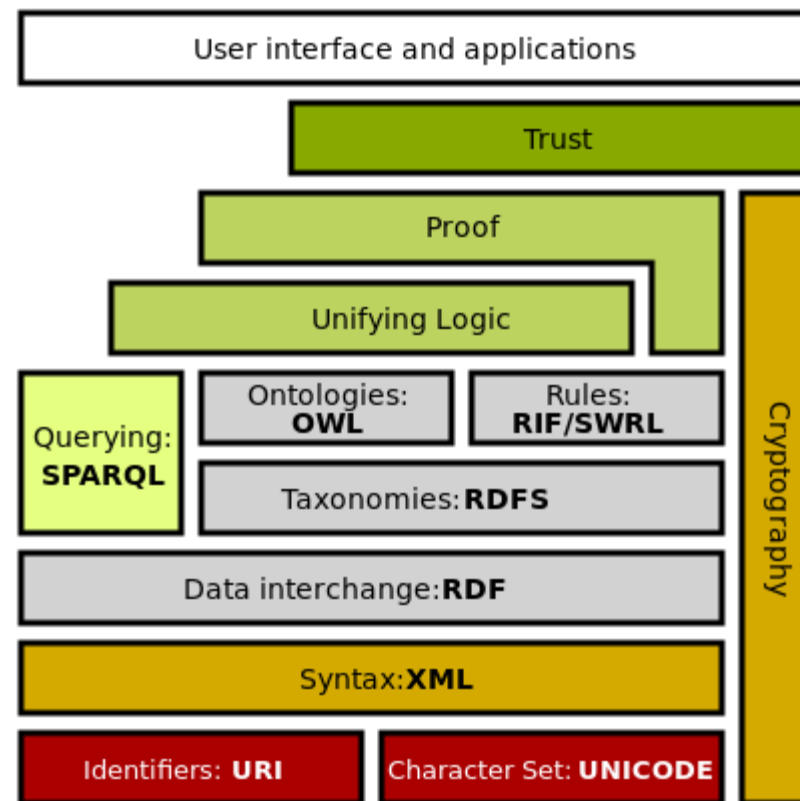
Limitations in available data will, in turn, impact capabilities of military personnel (e.g., commanders, analysts)



# The Semantic Web



- **Goals of the Semantic Web:**
  - Facilitate web-based publication and linking of machine-interpretable data
  - Support interpretation of data into actionable information, via logic-based knowledge encodings
- Prior IoT research has demonstrated utility of the Semantic Web for:
  - Dynamic Service Discovery [Chun, 2015]
  - Pervasive Computing [Jussi, 2014]
  - Context-Aware Asset Search [Perera, 2013]



**Will similar utility be realized under conditions imposed by Military C2 infrastructures?**



In establishing IoT for C2 operations, the following questions must be addressed:

- *Why are more sophisticated information processing methods needed for military IoT infrastructures?*
- *What types of service extensions should be applied to existing IoT middleware?*
- *What are the core research challenges that exist in facilitating these extensions?*

## **My Position:**

- New innovations in IoT middleware design are needed to support intelligent information integration and interpretation
- Semantics-based middleware extensions – relying on combined use of ontologies and Semantic Web technologies – offer significant promise



At present, effectiveness of semantic technologies in military networks still needs to be evaluated. Particular areas of interest include:

## **Distributed Dataset Access**

- Interpretation of Semantic Web data often requires access to distributed content
- Disrupted access to datasets or ontologies may impact real-time utility of IoT data streams

## **Management of Cloud-based Services**

- Processing-intensive tasks (e.g., reasoning) difficult to manage at tactical edge
- In commercial settings, cloud-based processing centers used, but significant bandwidth needed to send data to/from these centers



## Concluding Summary




- The Internet of Things offers several potential benefits toward C2 operations
- However, actionability of IoT-derived data and information may be threatened by several factors:
  - Limits on connectivity and processing capacity
  - Security / trust for IoT assets
- There is an established need for data semantics in IoT based services, which extends to C2 settings

### **Some Next Steps:**

- Implementation of semantics-based IoT services
- Evaluation of these services under resource-constrained networks



Michael Gerz  
Fraunhofer FKIE



Thomas Remmersmann  
Fraunhofer FKIE



*Michael Hieb, Ph.D.*  
C4I & Cyber Center  
George Mason University





# Why Do We Need Autonomy in Future Command and Control?

---

- ▶ Take advantage of offset technologies being currently developed
- ▶ Achieve better performance of robotic entities and systems
- ▶ Achieve mission goals with reduced risk, manpower and cost

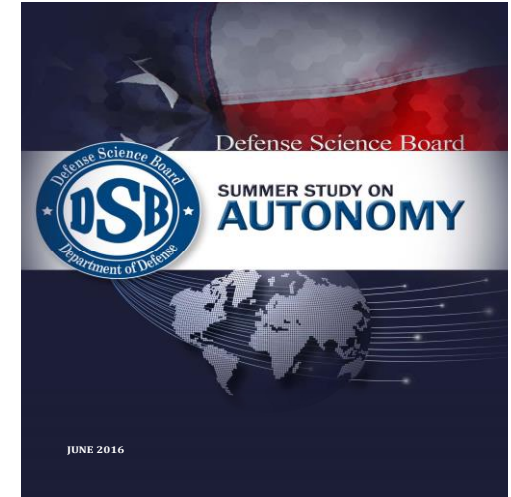


# Defense Science Board Summer Study on Autonomy – 2016

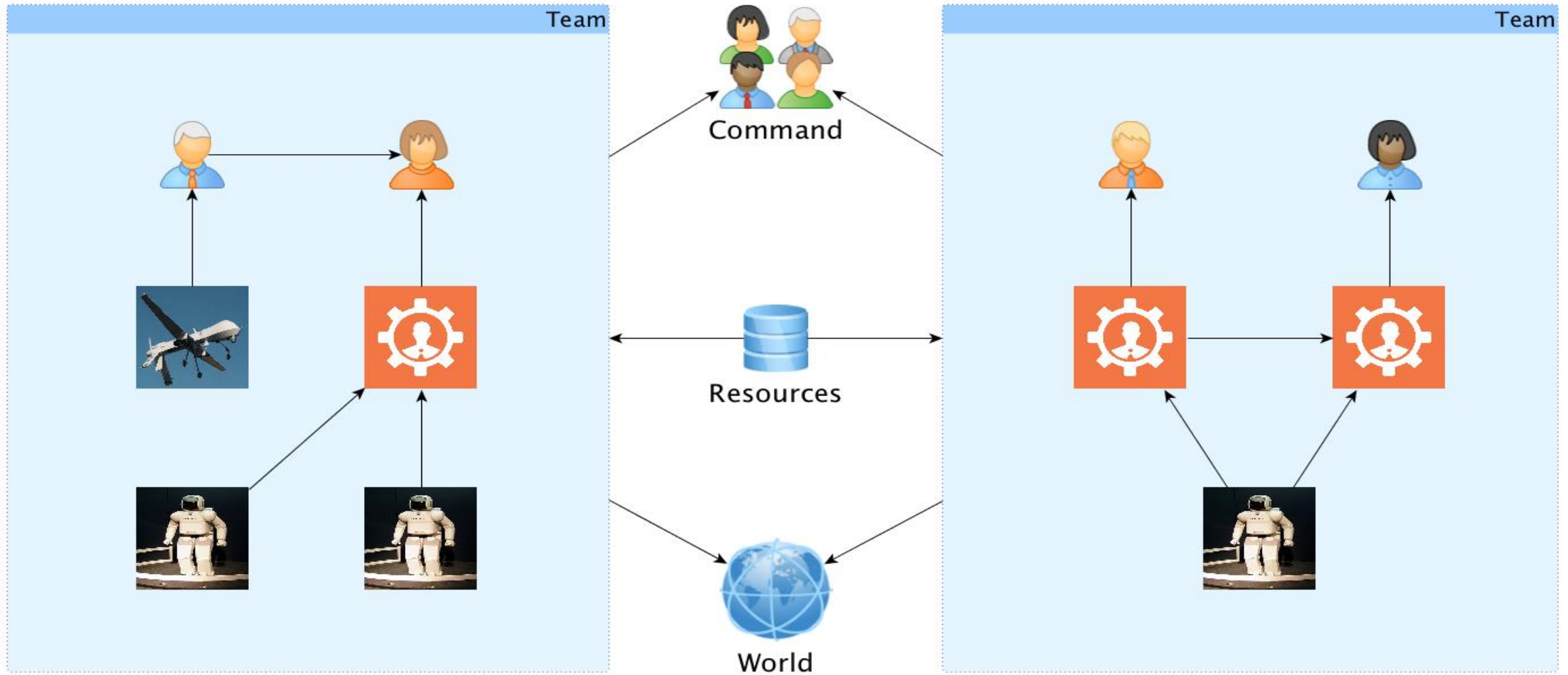
---

## *Value of Autonomy for addressing Operational Challenges*

- Rapid decision-making
- High heterogeneity and/or volume of data
- Intermittent communications
- High complexity of coordinated action
- Danger of mission
- High persistence and endurance



# Hybrid Military Operations



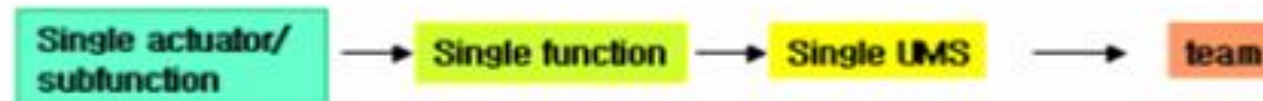
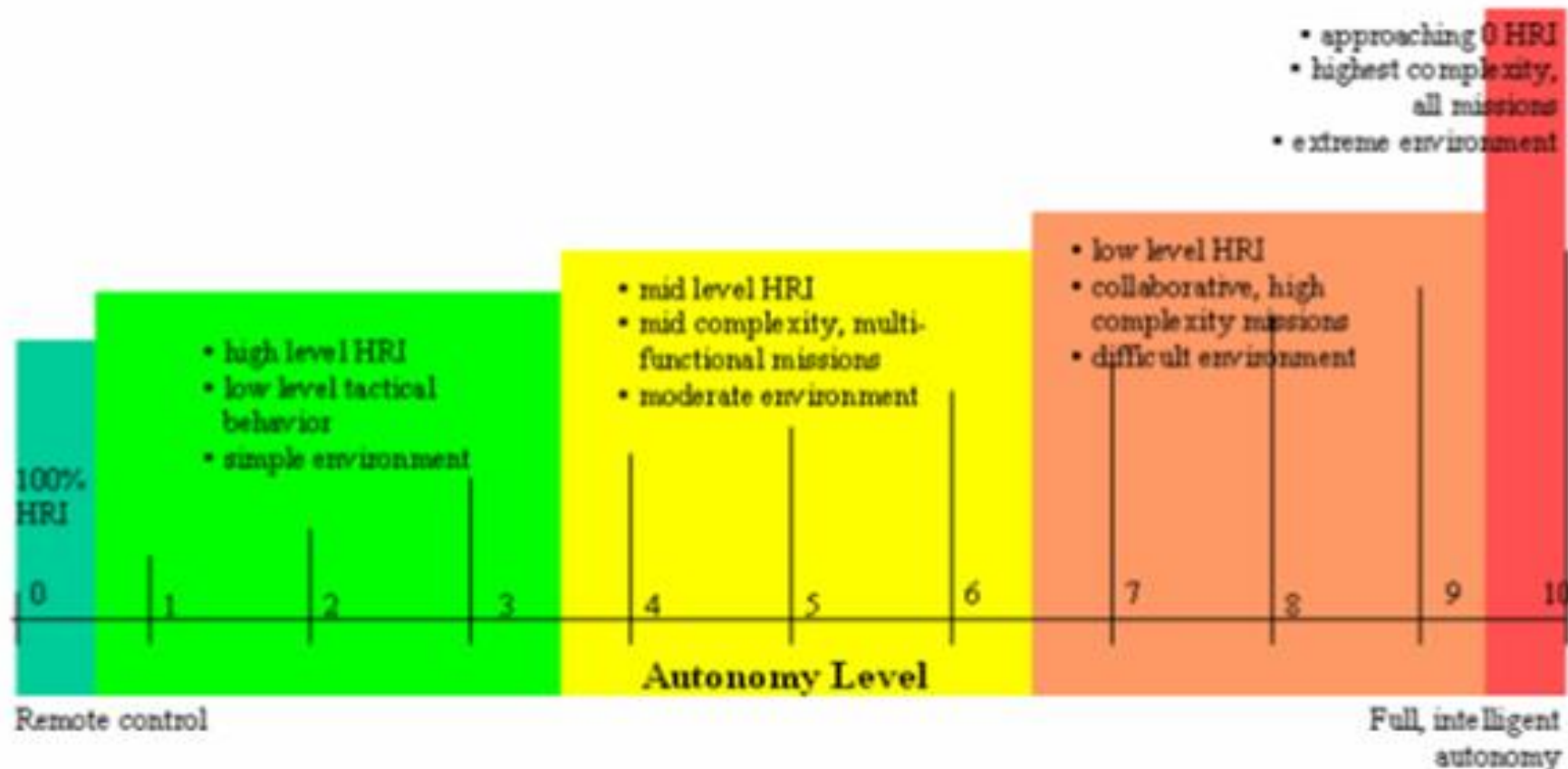
# Collaboration & Autonomy

---

- ▶ “Hybrid Teams” require interaction and collaboration in problem solving
- ▶ How can the IoT be included in these “Teams”?
- ▶ Need development of cognitive interfaces for non-human agents
- ▶ Research from Organizational Psychology (Multiteam Systems – Zaccaro et. al. 2012) is applicable
- ▶ Key problem is how to communicate Mission Goals and Intent



# Autonomy Level for Unmanned Systems (ALFUS)



# Key Autonomy Issues

---



- The need to build trust in autonomous systems while also improving the trustworthiness of autonomous capabilities
- The need to accelerate adoption of autonomous capabilities through DoD enterprise-wide enablers
- The need to strengthen the operational pull for autonomy by demonstrating operational value across a broad range of missions
- The need to expand the technology envelope to help the U.S. sustain military advantage through the increasing use of autonomy





Wrapping Up...

# Some Related Activities

---

- ▶ IEEE World Forum on Internet of Things – Special Session on Military Applications of IoT
  - ▶ <http://wfiot2016.ieee-wf-iot.org/program/special-session-on-military-applications-of-iot/>
- ▶ NATO IST-147 Research Task Group on Military Applications of IoT
  - ▶ BEL, FRA, GBR, GER, NLD, NOR, POL, ROM, TUR, USA and the NCIA

