Command and Control Research Challenges

30 October 2019

Craig Lawrence, PhD

Director, Systems Research

Applied Research Laboratory for Intelligence and Security (ARLIS)

UNIVERSITY OF MARYLAND

Outline

- Command and Control in the DARPA *Mosaic Warfare* Portfolio
  - Tactical Battle Management
  - Operational Level Command and Control
  - Cross-Domain Adaptation and Resourcing
- ARLIS Command and Control Research
  - ARLIS Introduction
  - Human-Machine Teaming

My Background

- Education
  - PhD, Electrical Engineering (Control Theory), University of Maryland, College Park
- Industry
  - 15 years at Alphatech, Inc., and BAE Systems
  - Managed group focused on defense and intelligence community research and development
  - Battle management, command and control (BMC2); autonomy and machine learning; optimization; control theory and estimation; and modeling and simulation
- Government
  - Program Manager (just under 6 years), DARPA Strategic Technology Office
  - Developed and managed the BMC2 Portfolio
  - Portfolio included five full programs, numerous studies, several SBIRs, a young faculty award, …
- Academia
  - Recently joined the University of Maryland's University Affiliated Research Center (UARC)

Command and Control in the DARPA *Mosaic Warfare* Portfolio

UNIVERSITY OF MARYLAND

The need for a pivot from Dominance to Lethality

Chinese J-31
Stealth Fighter

Russian PAK-FA
(T-50) Stealth Fighter

Russian SS-N-26 Cruise
Missile

North Korean
Musudan IRBM

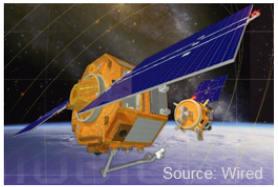
Chinese KJ-2000

Potential adversaries have advanced capabilities aligned against every one of our strengths.

Our systems are still better today, but…

Iranian Fateh-110
SRBM

Chinese PL-15
Missile



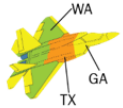
Chinese
Space Robotics

Russian S-400 IADS

IRBM: Intermediate Range Ballistic Missile
SRBM: Short-Range Ballistic Missile

The need for a pivot from Deliberate Inertia to Continuous Speed

19.1 years from contract to IOC



Initial ATF requirement

RFP issued

Lockheed contracted

YF-22 EMD first flight

contract

F-22 first flight

F-22 first delivered

Collier IOC trophy

First overseas deployment

Last F-22 delivered

'82 '84 '86 '88 '90 '92 '94 '96 '98 '00 '02 '04 '06 '08 '10 '12

IBM PC

Reagan: Star Wars

Gorbachev: perestroika

Berlin wall falls

USSR dissolved; Desert Storm

USB 1.0

Retaliation on Taliban

9/11 Attacks

Iraq invasion

iPhone

Lehman bankrupt

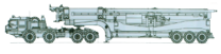
bin Laden dead

SA-10d

SA-12

SA-20

SA-21



SA-23

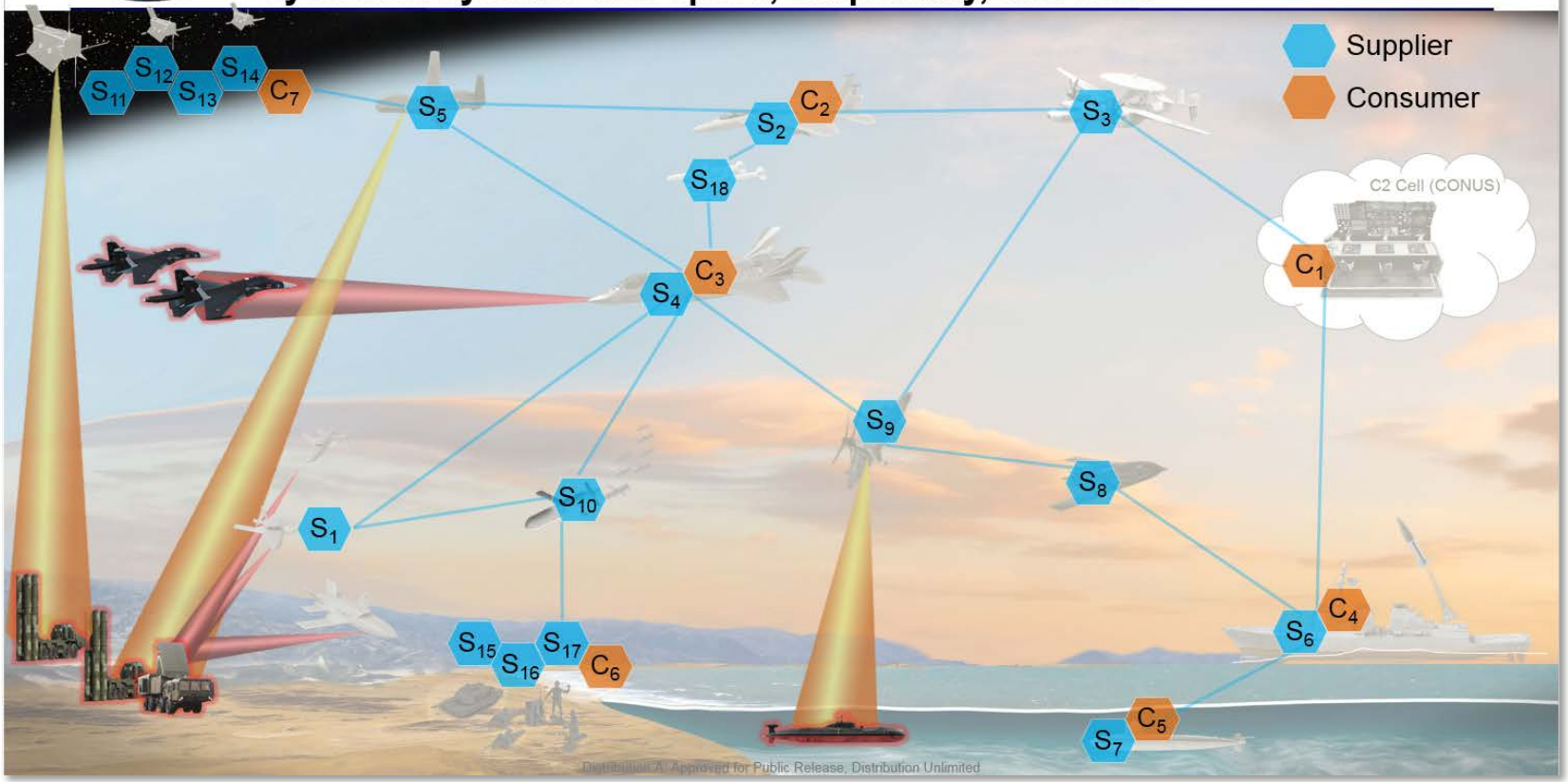
S-500

6 threat generations

Potential adversaries are significantly out-pacing us in development of new capabilities

They will eventually surpass us…

Mosaic Warfare:
System of Systems with speed, adaptability, and scale



Distributed systems must be Mosaic to win

© Kyoshino

pieces, interfaces painstakingly engineered
can only be assembled in one way

creates a distributed monolith
retains legacy vulnerabilities, introduces new set

© absolutearts

pieces, interfaces engineered for interoperability
can be assembled in many ways

creates an adaptable, resilient, distributed system
retains, improves legacy capability, mitigates vulnerabilities

What is needed for Mosaic Warfare?

Planning and Composition

- What is the objective? What effects do I want?
- How do I decide what to use and how to organize it?
- How do I know what is available?
- How am I going to use it? (i.e. What's the OPLAN?)
- How can I trust it?

Interoperability

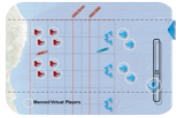
- How do things connect (new links)?

- How can I connect the right things (adaptive networks)?

- How do we work across security domains?

- How do machines understand each other?
- Can information drive the network? How can I discover nodes and links?
- How do I get capabilities into existing systems?
- Can we do better at testing and reliability?

Execution



- How do humans and machines share tasks at the edge?

- How do I re-allocate capabilities at combat speed?
- How do we develop fine-scale tactics automatically?
- How can we train human operators fast and minimize burden?

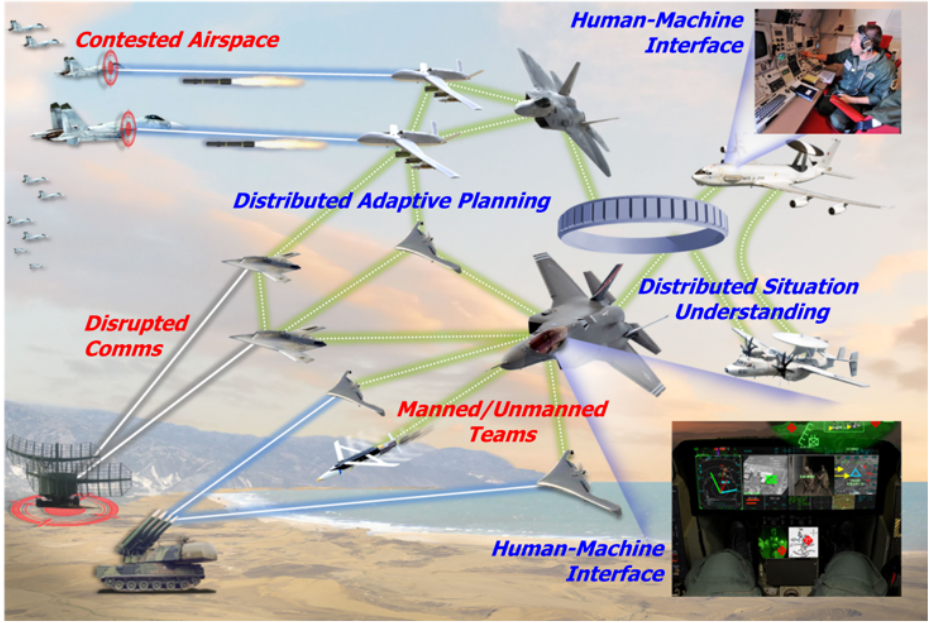
Distributed Battle Management

Problem: Increasing battle management challenges

- Attacks on battle management nodes
- Attacks on communications
- Large numbers of threats
- Increasing complexity
  - Manned/Unmanned teams
  - New technologies and CONOPS

Solution: Robust and reliable decision aids

- Distributed adaptive planning & control
  - Collaborative coordinated replanning
  - Optimized tasking and routing
- Distributed situation understanding
  - Common operational picture
  - Fused and shared data
- Human-led control
  - Flexible autonomy
  - From tactical platforms



Goal: Transform Tactical Air Battle Management

Distributed Battle Management

Tactical decision aid to support attack, intelligence, surveillance and reconnaissance (ISR) and other missions for manned/unmanned teams.

- Better understand the tactical situation for self, mission package, and area of interest
  - Tactical situation includes threats, targets, and status of assigned resources
  - Sensor and fused data from self sensor, wingman sensors and other external sources
- Planning options for multiple issues:
  - Pop-up high value threats/targets, loss of friendly assets, and other contingencies
  - Semi-automated plan/option generation in compliance with human-led priorities and guidance.
- Human interaction/displays that minimize the distraction and additional workload on the Flight Lead

Resilient Synchronized Planning and Assessment for the Contested Environment

- Context: Peer threat is driving a system-of-systems-based approach incorporating innovative technologies into future airborne architectures, e.g.,
  - Highly capable multi-role platforms combined with low-cost specialized platforms
  - Manned-unmanned teams and autonomy
  - Disaggregated capabilities (e.g., distributed EW, multi-static radar)

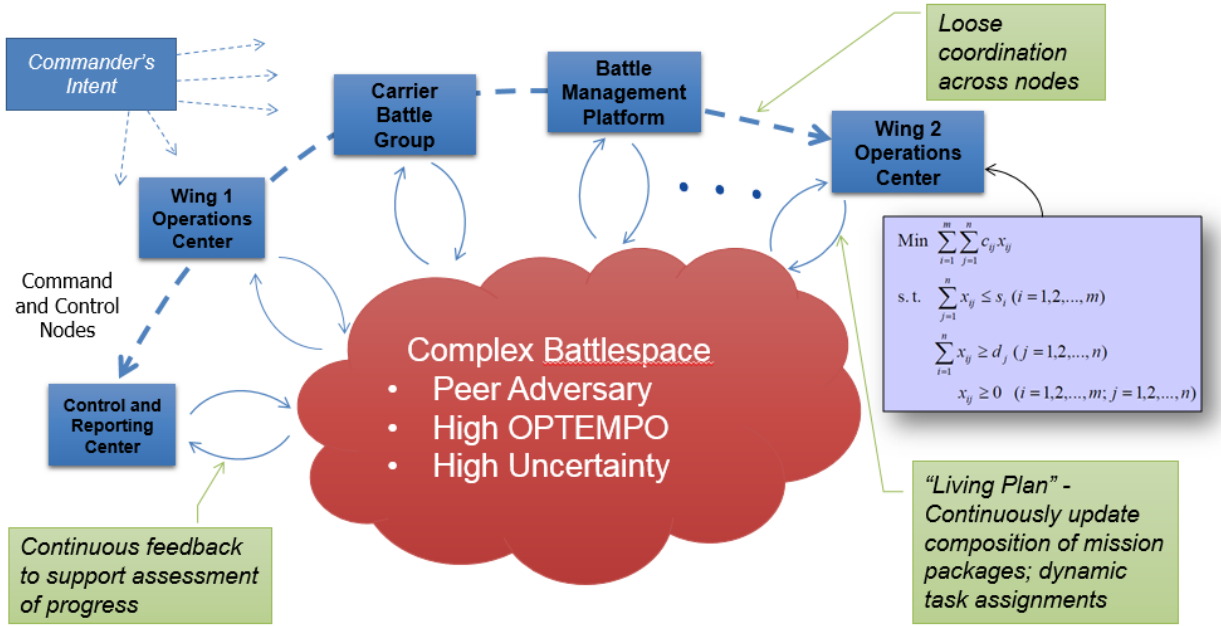
- Challenge: Highly contested environment threatens todays operations centers, limits or denies the use of space, degrades communications, and renders many traditional tactics irrelevant

- Program Objective: Operational-level command and control (C2) of current and future architectures ensuring continuity and maximizing effectiveness of air operations in a peer-threat contested environment
  - Command and Control - The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission (JP 1-02)

Robust C2 architectures and decision aids to maximize air campaign planners' ability to collaboratively coordinate plans consistent with commander's intent

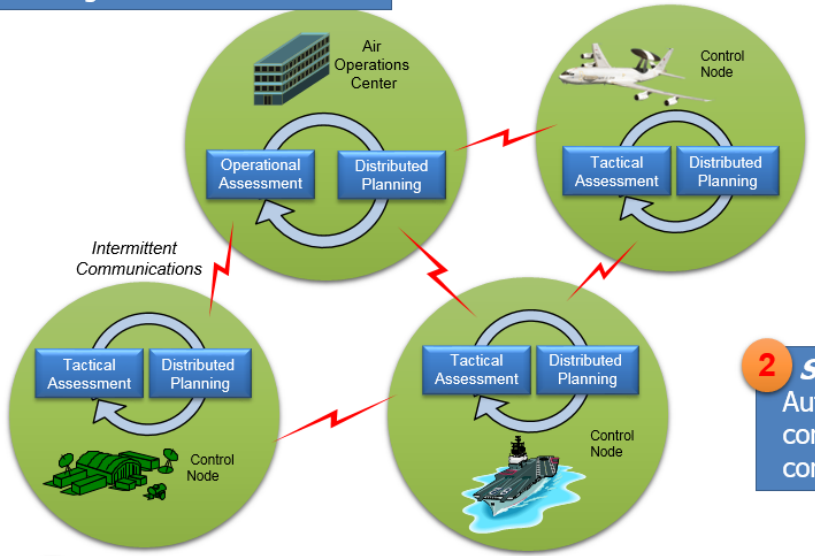
RSPACE Vision – Empowering Operators for Real-Time Distributed Planning

Human-centered tools for decentralized control of operations - A leap-ahead in resilience, responsiveness, and effectiveness



The RSPACE Solution – Helping Distributed Operators Control the Air Campaign

1 *Distributed Coordination*
Decentralize planning – enable agile coordination throughout the C2 network



- 10x + reduction in manning
- 10x + reduction in time
- Continuous operations in the face of uncertain C2 architecture
- Real-time adaptability of plans
- Integrate strike, ISR, and EW planning

2 *Scalable Automatic Planning*
Automation support to plan 1000s of complex interdependent missions – continuous updates to a "living plan"

3 *Human-Centered Automation*
User-adjustable level of automation - inject guidance and constraints during planning process

Services Recognize the Need for Multi-Domain Battle

…but today's command and control organization and processes cannot support the new warfighting concepts

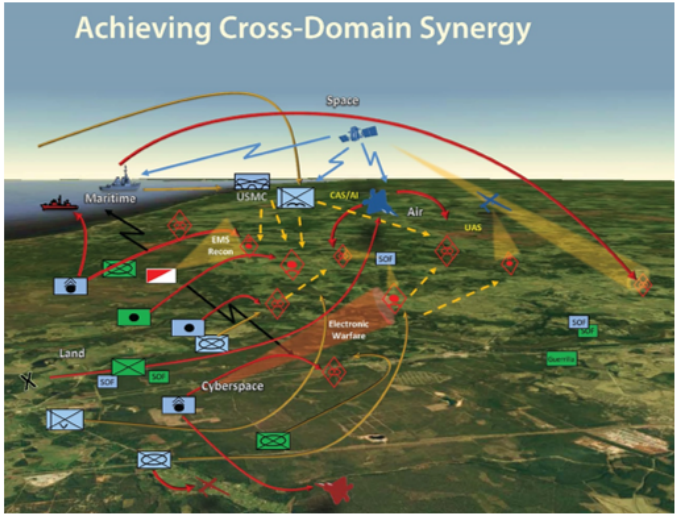
- Heterogeneous planning / control cells and manually-intensive processes limit multi-domain ops
  - Siloed hierarchical teams – coordination via **liaisons**
  - Statically allocated resources
  - Manual and slow
- E.g., air-land coordination in today's Air Operations Centers:

THEATER AIR OPERATIONS CENTER RELATIONSHIP

Coordinated, but not sufficiently *synchronized* to realize the full potential of multi-domain battle

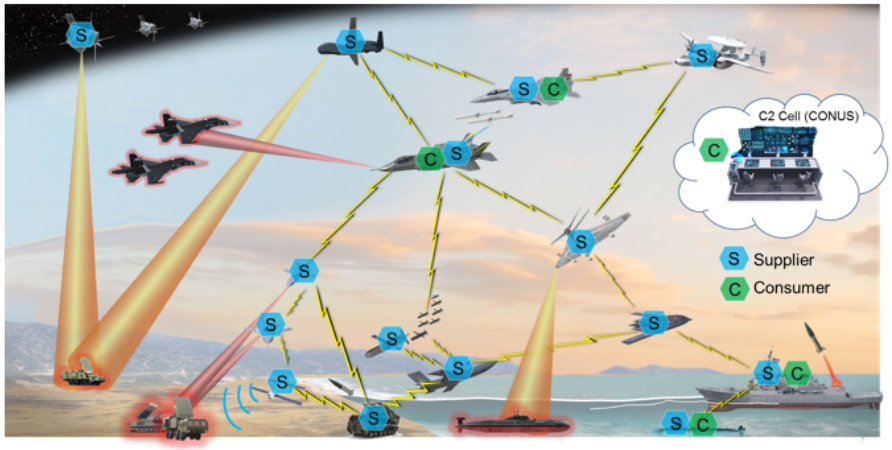
AOC – Air Operations Center
BCD – Battlefield Coordination Detachment
GLD – Ground Liaison Detachment
ICC – Installation Control Center
RLD – Reconnaissance Liaison Detachment

From GEN Perkins, "Multi-Domain Battle - Driving Change to Win in the Future," *Military Review*, July-August 2017



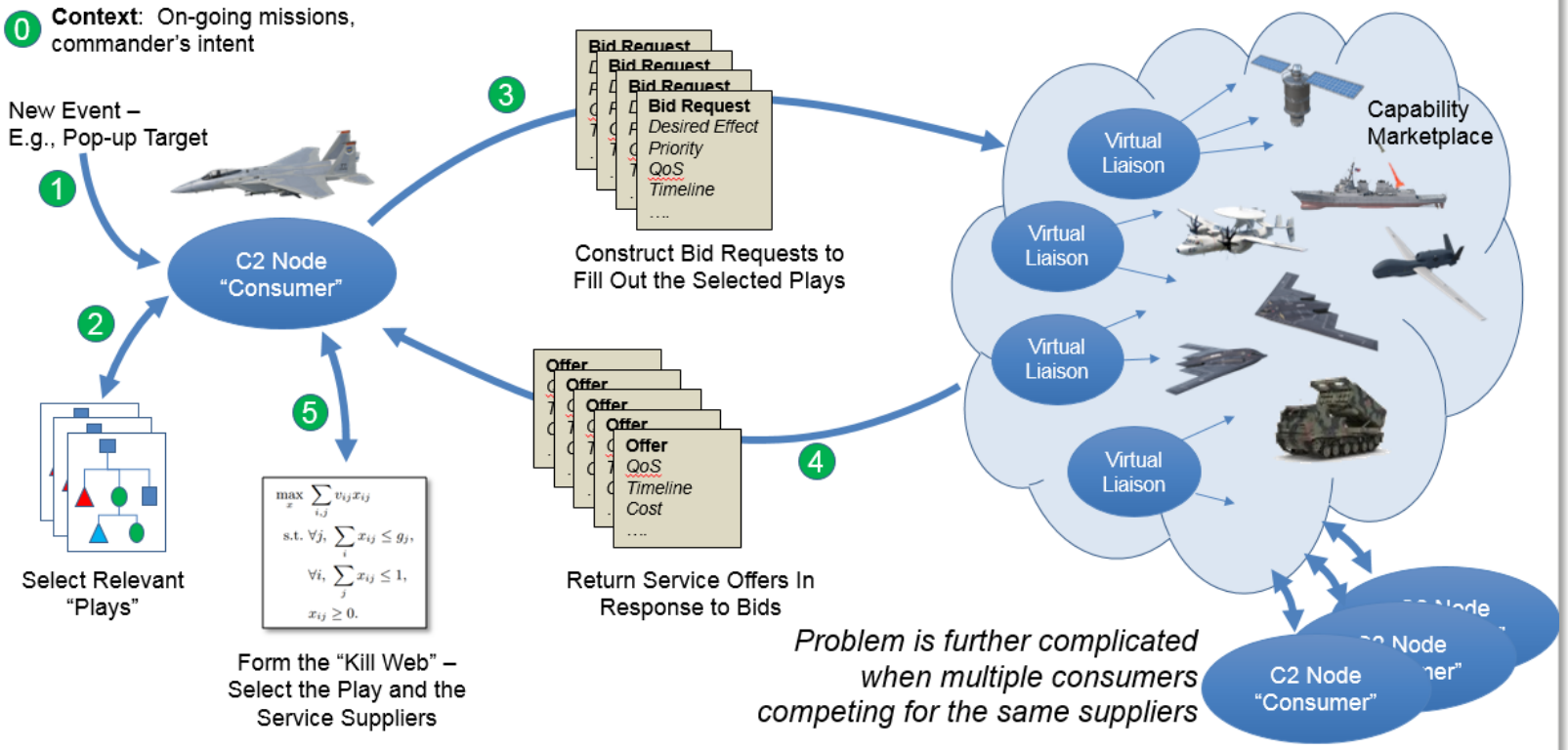
Adapting Cross-Domain Kill-Webs (ACK)

- Proposed framework – *Virtual Liaisons* and the *Capability Marketplace*
  - *Capability Marketplace* - All nodes across all domains are potential "suppliers"
  - Command and control nodes ("consumers") connect with suppliers via *virtual liaisons*
  - Virtual liaisons may be at the platform level, unit level, or higher – as appropriate
  - Negotiate the use of services to achieve effects in the context of on-going missions



Matching Effects Suppliers with Needs to Build Cross-Domain Kill Webs

Approach - Decentralized Construction of Kill Webs



Technical Challenges

Commerce Analogy Only Makes Sense When Suppliers are Readily Discovered and Bids and Offers can be Expressed in a Common "Currency"

- Challenges
  - In real-time (and to a large extent at planning time), little or no insight into what capabilities are available and what capacity they may have
  - Multiple commanders and missions across domains - no mechanism for assessing "value" / "cost" of supporting a new mission versus your current mission
  - Given a set of cross-domain kill web options, no mechanism for building and comparing diverse options and selecting the "best"
- Suppliers - the **virtual liaisons**
  - Develop language for defining services, expressing effects, quality of service, etc.
  - Assessing dynamic impact and **cost** of fulfilling a bid with respect to baseline missions / guidance
- Consumers – building the kill web
  - Selecting appropriate plays / plan templates
  - Constructing the "bid requests" in terms of desired effects (as flexible as possible), timelines, quality of service desired, …
  - Selection amongst the received options based on QoS / success probability estimates, costs, …
- Architecture and CONOPS
  - Distributed implementation – software infrastructure, multi-level security, …
  - Mechanisms for managing authority and service exposure based on conditions and rules of engagement

Command and Control at the Applied Research Laboratory for Intelligence and Security

CENTER FOR ADVANCED STUDY OF LANGUAGE

has become

APPLIED RESEARCH LAB FOR INTELLIGENCE AND SECURITY

As of 2018: New Sponsor
Office of the Under Secretary of Defense for Intelligence

in coordination with
USAF Office of Concepts, Development & Management

New Operating Model

- Project funds from across DoD and Intelligence Community
- A consortia-based model, engaging campus and beyond

Leveraging the full scope of the State of Maryland system of higher education to be the Nation's resource for translational and applied research for Intelligence and Security.

Human & Social Systems

- Human Behavior & Risk
- Culture, Language & Communication
- Competition Conflict & Security

Augmentation & Human System Integration

- Autonomy & Artificial Intelligence
- Human Performance & Learning

Information Engineering & Advanced Computing

- Information Dominance & Decision Analytics
- Translational Research & Technology

In line with sponsor priorities, the UARC will move away from a language focus and concentrate on issues related to **human behavior**, **human-machine interactions**, **artificial intelligence** and **leveraging new computing tools, techniques and platforms**.

ARLIS Vision Statement

1. The premiere strategic research partner for the DoD for the most critical and challenging intelligence and security problems that involve social and human systems.
2. Exploit social systems, autonomy and augmentation, and advanced computing to enhance day-to-day job performance as well as critical leadership decisions that affect missions success.
3. Nurture a dynamic network, and pipeline, of performers and early-career talent to accelerate discovery and innovation in critical national security areas.
4. Lead the University of Maryland, and the broader State of Maryland, in providing service to the United States Department of Defense and Intelligence Communities

ARLIS…

1. Serves (reports to) the Director for Defense Intelligence, Counterintelligence, Law Enforcement & Security
   - Areas: Security, Counterintelligence, Personnel, Industrial security
2. Supports the mission of OUSD(I) and DoD IC
   - Areas: Policy, ISR, Battlespace Awareness, HUMINT, partner engagement, DoD IC agencies (NGA, ONI, DIA, NSA, NRO)
3. Serves the IC and DoD community
   - More broadly: FBI, ODNI, CIA, IARPA, DARPA, Army (C5ISR, CSC), Navy (NAWCAD, USNA), Air Force, NNSA (NA-12; NA-10) in ways that leverage and enhance the UARC core competencies

ARLIS Integration with Campus

Augmentation & Human System Integration

UMIACS
University of Maryland
Institute for Advanced
Computer Studies

MARYLAND ROBOTICS CENTER

BBI
Brain and Behavior Initiative

UNIVERSITY OF MARYLAND
COLE FIELD HOUSE

HCIL

The Institute for Systems Research

MAVRIC
Mixed Augmented/Virtual Reality
Innovation Center

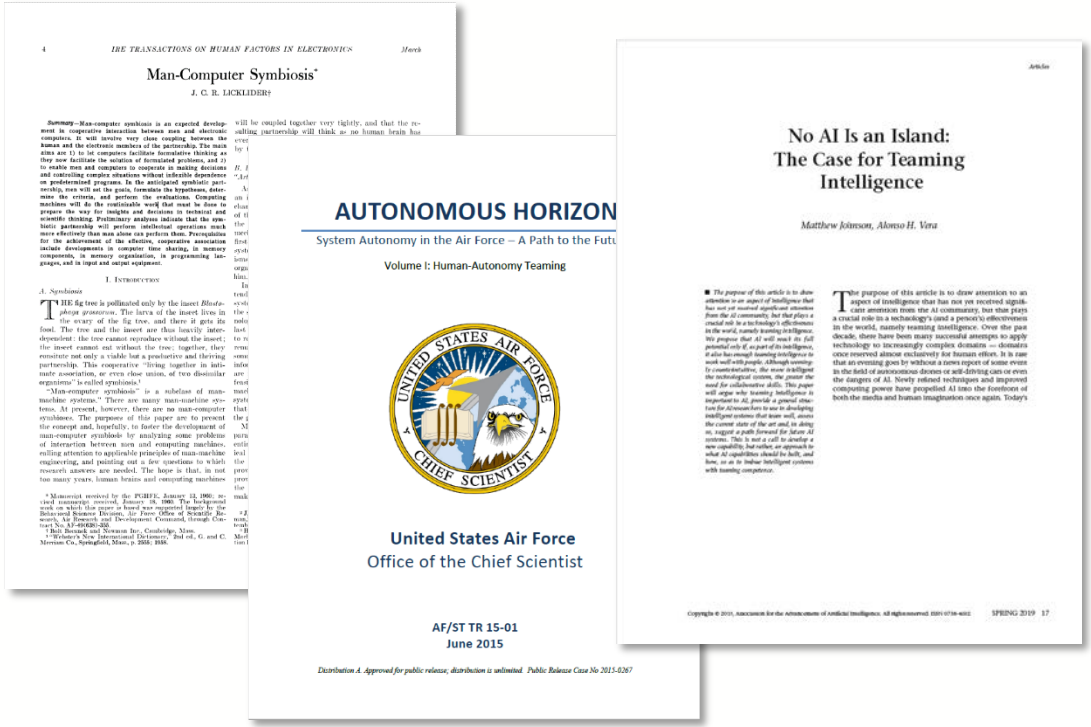
PIRL
Perceptual Interfaces &
Reality Laboratory

Evolving Disruption Strategy

1. **Human-Machine Symbiosis**:
   How far can we integrate humans and machines?
   i.e., VR/AR and AI+HCI, AI “Systems Engineering”, novel interfaces
2. **Influence and Behavior**: *How do we detect and deflect cognitive and societal attacks?*
   i.e., information operations, disinformation, deep fakes, insider threat, personnel vetting, etc.
3. **Advanced sensing**: *How deep can we sense?*
   i.e., vision, perception, quantum, humans, groups, society, etc
4. **Industrial resilience**: *How to deliver uncompromised?*
   i.e., 5G testbed, industrial security, supply chains, cyber, etc

Human Machine Teaming

- Goal: “Man-Computer Symbiosis” (J.C.R, Licklider, 1960)
  - Humans and machines in a partnership that “…will think as no human brain has ever thought and process data in a way not approached by … machines…”
- Claim: Effective teams are built on *trust*, *common understanding*, and appropriate *allocation of roles*



Human Machine Teaming Challenges

- Trust
  - “Explainability” of plans and decisions
  - “Directability” for planning and autonomy
- Common Understanding
  - Intent – both for the human and the machine
  - Shared situation awareness
  - Common language for **interaction** – incl. effective communication of state, AR/VR interfaces
- Role Allocation
  - Appropriate assignment of roles to humans and machines
  - Adaptation based on context
  - Avoid the “Automation Conundrum” (Endsley, 2017)

Project CAVES: Collaborative Analysis in a Virtual Exploration Space

- Goal: Develop augmented reality / virtual reality (AR/VR) prototypes for collaboration
  - Immersive collaborative environment, explicit incorporation of participants, realism
- Challenge Problem
  - Planning and rehearsal for across distributed command posts
  - Provide similar experience to collocated planning and rehearsal
  - Working with Army Futures Command CCDC/C5ISR Center
- State of the Art: Electronic sand tables, collaborative environments on 2-D displays

Current State of the Art:
Command Post of the Future (CPOF)
Interactive, 2D, collaborative COP

CAVES Challenges

- Operational
  - Same space, different locations
  - Austere environments and interconnectivity
  - Information transmission and receiving
  - Multi-domain visualization with cyber patterns & emissions
  - Human factors and workflow
- Design
  - Improve sensory vividness and efficiency
  - Minimalize sensory overload
  - Reduce cyber sickness
  - Individualized Human Factors in AR/VR Performance metrics
  - VR/AR Familiarity

Augmented Reality & Heat Mapping