Emerging Technologies: Test and Evaluation Implications

Dr. Greg Zacharias
Chief Scientist
Operational Test and Evaluation
Office of Secretary of Defense

10 April 2019
DOT&E Focus Areas

- Dealing with Software Intensive Systems and Cybersecurity
- “Shifting Left” with Combined Testing and Rapid Acquisition
- Improving/Enhancing Our Test Environments
- Recognizing Importance of Human-System Integration
- Increased Modeling & Simulation and Move to Digital Engineering
- Assessing Reliability’s Impact on Sustainability
- Adapting T&E for Emerging Technologies
- Maintaining an Agile Workforce
Adapting T&E for Emergent Technologies

- **Hypersonics and Directed Energy**
  - Just “range” and “range safety” issues, or deeper implications for T&E?

- **Quantum Computing and Communications**
  - Dealing with fundamental uncertainty

- **Nanomaterials and additive manufacturing**
  - What are implications for reliability and sustainability evaluation?

- **Autonomous Systems**
  - These systems can and will be complex, and can fail in multiple subtle ways
  - They may also “learn” new behaviors over time and/or over the system population, changing their capabilities dynamically
  - We’ll need to design for testability, beginning with requirements specification in several areas
  - New approaches to T&E will be required as well
Why Autonomous Systems?

- **Operational Pull**
  - Now facing near peer adversaries who are catching up with our 1980’s “second offset” investments
  - Can’t keep pursuing risk-averse incremental improvements
  - Need a “third offset” to move from industrial age to information age, making better and quicker decisions, and increasing end-point lethality

- **Technology Push**
  - Autonomous Systems (AS) and foundational Artificial Intelligence (AI) technologies are growing at a dizzying pace
  - And computational infrastructure is as well: computational power, memory, networking, and datasets

- **Benefits**
  - Yes, robotic autonomous platforms for sure. But much more than that: large-scale multi-sensor fusion and assessment, rapid and accurate decision-aiding/making, and coordinated multi-domain effects delivery
  - Our current platforms will become peripherals for a knowledge-based AS-enabled information-age force
Autonomy: What is it?

- The formal definition (Merriam-Webster)
  - The state of existing or acting separately from others

- Typical working definition (in personnel context)
  - A degree or level of freedom and discretion allowed to an employee over his or her job [note: not complete freedom]

- Broken down for working with machines
  - WHAT to do (goals/objectives, or mission)
  - WHAT NOT to do (constraints, or Rules of Engagement (ROEs))
  - And maybe some of the WHYs (supervisor/commander intent)
  - But not details on HOW to do it (methods) nor HOW to deal with “unplanned for” conditions (eg, dealing with adversary)

- And recognize that these machines can be either*
  - “In Motion” (ie, robots, future UUVs)
  - “At Rest” (ie, cyberwarriors, logistics planners, etc)

* Defense Science Board, 2012
The time is right. Why aren’t we moving more quickly?
Yes, our efforts are scattered, stovepiped, duplicative, and lacking critical mass…but what else is missing?
Do we care how these systems are defined or is it more important how they behave?
Can we bring disparate communities together with common frameworks, architectures, and “challenge problems” all can work on and contribute to?
Most critically, what are the key T&E issues we face, and how can we best deal with them, both from a system design point of view, and via T&E tools and processes?
Properties for Proficiency

- **Situated Agency**
  - “Sensing” the environment, assessing the situation, reasoning about it, making decisions to reach a goal, and then acting on the environment
  - Forming a closed loop of “seeing/thinking/doing” iteratively and interactively with the environment

- **Adaptive Cognition**
  - Using different modes of “thinking”, from low-level rules, to high-level reasoning and planning, depending on difficulty of the problem, and need for flexibility in dealing with unexpected situations

- **Multi-Agent Emergence**
  - “Interacting” with other agents, human or otherwise, giving rise to emergent behavior of the group/team, not necessarily contemplated in original “local” autonomous system design

- **Experiential Learning**
  - “Learning” new behaviors over time and experience, by modifying internal structures/parameters to improve performance in terms of one or more performance metrics (eg, task optimality, error robustness,...)
Autonomous decisions can lead to high-regret actions, especially in uncertain environments
- Trust is critical if these systems are to be used, and not ignored

Barriers to trust in autonomy include those normally associated with *human-human* trust
- Proficiency, integrity, dependability, predictability, timeliness,…

But there are additional barriers to *human-machine* trust:
- They don’t “think” or “talk” like we do, they can’t explain themselves, they have low self-awareness,…

So what happens? Humans behave as if they’ve received the following advice:

> Never trust anything that can think for itself if you can't see where it keeps its brain.*

*Harry Potter and The Chamber of Secrets, J. K. Rowling, 1999*
Tenets of Trust

- Enable “cognitive congruence” with transparency
  - Architect the system at high level to be congruent with the way humans parse the problem
  - Provide for explanation of reasoning, from perception, to goal generation, to action selection
  - If the system can’t explain its reasoning, then the human teammate should be able to drill down and trace it
- Ensure situation awareness of self and environment
  - Provide knowledge base for environment and mission awareness
  - Provide information on system health and location in design envelope
- Support effective human-system integration
  - Enable mutual understanding of common/complementary roles/goals
  - Support ease of communications between humans and systems
- Enable human-system teaming and training
  - Conduct extensive human-system team training, to develop mutual mental models of each other, across range of missions, threats, environments, and users
Principles of Flexibility

- **Task Flexibility**
  - Change AS task or goal taken on, depending on the overall mission and situation
  - Enabled by fundamentals of situated agency, interacting with the environment, task-sharing with other agents (human or machine) on its team, learning from experience…and trust

- **Peer Flexibility**
  - Take on subordinate, peer, or supervisor roles with other agents as necessary, and understand the meaning of the new peer relationship
  - Enabled by the fundamentals of situated agency, learning from experience, multi-agent emergence…and trust

- **Cognitive Flexibility**
  - Change how a task is carried out, by assessing a technique’s contribution to task performance in a given situation and mission, selecting among several, or “voting” across many
  - Enabled by the fundamentals of adaptive cognition and learning from experience…and trust
Proficiency and Trust
Ensure Flexibility

Properties for Proficiency
- situated agency
- multi-agent emergence
- experiential learning
- adaptive cognition

Principals of Flexibility
- peer flexibility
- task flexibility
- cognitive flexibility

Tenets of Trust
- cognitive congruence
- situation awareness
- human-system integration
- human-system teaming/training

AUTONOMOUS BEHAVIOR
Behavioral Objectives for ASs

- **Ensure proficiency via...**
  - ...situated agency in the environment and team, capacity for adaptive cognition, allowance for multi-agent emergence, and ability to learn from experience

- **Ensure trust via...**
  - ...cognitive congruence and transparency of decisions, situation awareness, natural human-system interaction, and effective human-system teaming and training

- **Ensure flexibility in terms of...**
  - ...an ability to change *tasks* depending on mission/situation, change *roles* and peer relationships with other agents, and change *how to accomplish* a task, based on situation and experience
Unifying Frameworks, Architectures, and Platforms

- **Convergence of communities**
  - Robotics, cybernetics, cognitive psychology, neuroscience, traditional “hard” AI, emerging “soft” AI

- **Common frameworks and architectures**
  - Computational models of perception, cognition, and action
  - Research, development, and operational benefits
  - Functions: sensing, fusion, deciding, planning,…
  - Techniques: traditional algorithms, machine learning,…

- **Platforms**
  - Computational infrastructure: computational nodes, memory, networking, and datasets
  - Knowledge Platform: integration at the enterprise level
Convergence of Communities

- Robotics
- Cybernetics
- Human-systems teaming
- "Hard" AI
- "Soft" AI
- Cognitive psychology
- Cognitive architectures
- Neurosciences

Common Framework for Autonomous Systems

Cognitive computational models of humans and for systems
Common Framework for Autonomous Systems

Human Computer Interfaces (HCIs) & Collaboration Environments

Sensors

Sensor/Data Fusion

Sensor Management & Data Mining

Databases

Situation Assessment and Decision-Making Layer

Learning & Adaptation Layer

Domain-Specific Knowledge Base Layer

Toolsets & Technologies Substrate
Key Functions & Techniques/Toolsets

AS Functions

- Sensor/data fusion
- Perception and event detection
- Situation assessment
- Reasoning and decision making
- Planning and replanning
- Execution management
- Learning and adaptation
- Knowledge maintenance and sensor management

Enabling Techniques/Toolsets

- **“Hard” AI**
  - Symbolic Processing
  - Logic Programming
  - Expert Systems
  - Knowledge Representation

- **“Soft” AI**
  - Artificial Neural Networks
  - Evolutionary/Genetic Algorithms
  - Fuzzy Logic
  - Bayesian Networks
  - Probabilistic Programming Languages

- **Machine Learning**
  - Classification & Cluster Analysis
  - Decision Tree Learning
  - Regression Analysis
  - Support Vector Machine
  - Statistical Learning Theory

- **“Traditional” Methods**
  - Systems Identification
  - Estimation and Control Theory
  - Optimization
  - Multi-Agent Systems
AS Architectural Pattern

- Human-Computer Interface
- Autonomous System Architecture
- Computational Methods/Algorithms
- Hardware/Software Platforms
- sensors
- effectors

OUTSIDE WORLD
Architectures & Technologies

- Develop one or more *common AS architectures*
  - Provide for end-to-end “see/think/do” functionality, bridging gaps across different communities, separating functionality from technology, and ensuring extensibility and reuse

- Pursue development of *enabling technologies*
  - Pursue – from basic research to exploratory development – technologies that can support the “see/think/do” functions, learning/adaptation, knowledge-base management, and human-computer interfaces

- Develop and promulgate a *multi-tiered hardware and multi-layered software architecture*
  - Embrace modern hardware/software architectural design patterns to take full advantage of emerging technology trends, particularly in the commercial sector
T&E Concerns: Some Studies

- D. J. McMorrow, *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD*, JSR-16-Task-003, The MITRE Corp, McLean, VA, 2016
- B. Haugh, D. Sparrow, and D. Tate, *The Status of Test, Evaluation, Verification, and Validation (TEV&V) of Autonomous Systems*, P-9292, Institute for Defense Analysis, Alexandria, VA, 2018
AS T&E Issues Raised

dynamic, unpredictable, & unstructured environments
astronomically large state space
inability to specify requirements at an operational level
lack of frameworks/architectures
emergent behaviors within & across ASs
human trust of ASs (and vice versa)

non-deterministic behaviors
no instrumentation or design for “testability”
lack of evolution of CONOPs with AS development
lack of T&E ranges, testbeds, personnel
dealing with learning, pre- and post-fielding

lack of understanding AS internals (perception, cognition,...)
formal methods, classical stats lacking
no requirements traceability through CT/DT/OT
subjective risk assessments uninformed by data
inadequate HSI, comms

and other stuff I forgot to put on this slide
Some grey clouds can be dissipated by design principles for proficiency, trust, and flexibility.

But we need some additional bursts of sunlight.

- OP reqmnts $\rightarrow$ component reqmnts
- Design for testability
- Transparency/explainability
- Run-time monitor
- Sequential T&E throughout life cycle
- "Aggressive" use of M&S
- Co-develop CONOPS with AS
- New methods for dealing with emergence, learning
- Improved stat engineering methods
- Data- and argumentation-based risk traceability

AS T&E Recommendations
Director, Operational Test and Evaluation

Thanks!
DOT&E Organization

Director, Operational Test and Evaluation
HON Robert F. Behler
703-697-3655

Principal Deputy
Mr. David Duma
703-695-2912
david.w.duma.civ@mail.mil

Senior Military Assistant
CAPT John Roussakies, USN
703-697-3655
joannis.c.roussakies.mil@mail.mil

Deputy Director, Land and Expeditionary Warfare
Mr. Steve Daly
703-697-3891
stephen.c.daly.civ@mail.mil

Deputy Director, Air Warfare
Mr. Mike Crisp
703-692-1708
michael.d.crisp2.civ@mail.mil

Deputy Director, Live Fire Test and Evaluation
Dr. Sandra Ugrina
703-614-5408
sandra.ugrina.civ@mail.mil

Deputy Director, Naval Warfare
Dr. Ray O'Toole
571-372-3873
raymond.d.otoole1.civ@mail.mil

Deputy Director, Net-Centric, Space, and Missile Defense Systems
Dr. Mitch Crosswait
571-372-3804
kenneth.m.crosswait.civ@mail.mil

Deputy Director, Land Warfare Systems
Expeditionary WF System
Battle Command
Land Munitions
Rotary & Tilt-Rotor Aircraft
Tactical UAV
Chem-Bio Defense Program
T&E Threat Resource Activity

Deputy Director, Air Combat Systems
Strategic Air Combat Systems
Aircraft Carriers
Air Launched Munitions
Endurance UAVs
Air Warfare C4ISR Systems
IR/UV/RF Def Combat Sys
Airlift Systems
Joint T&E Program
Center for Countermeasures

Deputy Director, Live Fire – Land, Air, Naval Lethality & Survivability
Joint Live Fire Program
Joint Aircraft Survivability
Joint Technical Coordinating Group-Munitions Effectiveness

Deputy Director, Surface Ships
Submarines & UUVs
Navy Combat Systems
Radars/CEC
Sonars
EW System
Naval Munitions
Missiles
Torpedoes
OT Infrastructure, Resources

Deputy Director, Space & Strategic Systems
Net-Centric Systems
Strategic C4ISR Systems
Major Automated Info Syst.
Chemical Weapons Demil
Ballistic Missile Defense Syst.
Cybersecurity Assessment Program

Senior Advisor for Software and Cybersecurity
Dr. Amy Henninger
703-697-4818
amy.e.henninger.civ@mail.mil

Chief Scientist
Dr. Greg Zacharias
703-695-2912
greg.l.zacharias.civ@mail.mil

Principal Deputy
Mr. David Duma
703-695-2912
david.w.duma.civ@mail.mil

3/19/19
Backups
What Would a Common Framework Buy Us?

- Provide common structures for many autonomous systems…
  - Internal component functions, their relationship to each other and the environment, and principles governing their design
- …to support parallel development efforts in different areas
  - Different groups can work complementary subsets of the problem, connecting with one another via the framework
- Develop unifying “science of autonomy” across 1000’s of “one-offs” now in the engineering community…
- …and point to where the S&T community needs to invest
  - Develop missing or inadequate functionalities
- Serve as foundation of an AS Open Systems Architecture (OSA)…
  - Encourage reuse of developed modules across applications
- …and support interoperability across DOD
  - eg, AF ISR UAVs cooperatively teaming with Navy attack UUVs
Autonomous Horizons II: Bottom Line

- Time is right for developing/fielding autonomous systems (AS)
  - Operational needs, technology advances, and transformational potential
- Need to specify general behavioral objectives
  - Proficiency, trust, and flexibility of operations
- S&T community needs to think more broadly
  - Common conceptual frameworks, unifying functional architectures, enabling technologies, and modern computational infrastructures
- But “non-technical” issues also need addressing
  - Challenge problems, both foundational and operational
  - Development processes including people, systems, data, and computational environments
  - Organizational structures for research and prototyping
- The potential is there to move us from a vehicle platform-centric organization to a holistic information-age enterprise

An agile information-centric enterprise making timely decisions executed via friction-free access to exquisitely effective peripherals
DoD Autonomy COI: Challenge Areas

Machine Perception, Reasoning and Intelligence (MPRI):
- Common Representations and Architectures
- Learning and Reasoning
- Understanding the Situation/Environment
- Robust Capabilities

Human/Autonomous System Interaction and Collaboration (HASIC):
- Calibrated Trust
- Common Understanding of Shared Perceptions
- Human-Agent Interaction

Scalable Teaming of Autonomous Systems (STAS):
- Decentralized mission-level task allocation/assignment
- Robust self-organization, adaptation, and collaboration
- Space management operations
- Sensing/synthetic perception

Test, Evaluation, Validation, and Verification (TEVV):
- Methods & Tools Assisting in Requirements Development and Analysis
- Evidence based Design and Implementation
- Cumulative Evidence through Research, Development, Test, & Evaluation (RDT&E), Developmental Testing (DT), and Operational Testing (OT)
- Run time behavior prediction and recovery
- Assurance Arguments for Autonomous Systems
Robotics
- ~1900’s: Remote control of torpedoes, airplanes
- 30’s – present: “Open loop” in-place industrial robots
- 40’s – 70’s: Early locomoting robots
- 70’s – present: “Thinking” locomoting robotics
  - Actionist approach (eg, Brooks’ iRobot, Google Cars, …)
  - Sensor-driven mental models of “outside” world; drive to “cognition”

Cybernetics
- 1940’s: *The scientific study of control and communications in the animal and the machine* (Norbert Weiner)
- 50’s – 70’s: Manual control (eg, flight simulators)
- 70’s – 90’s: Supervisory control (eg, FMS)
- 90’s – present: Cognitive models with a systems bent (e.g., COGNET, SAMPLE)
Cognitive Psychology

- The study of mental processes like attention, memory, perception, problem solving, language,…
- 50’s and 60’s: Broadbent attention theory, Chomsky’s theory of language, Newell/Simon Theory of Human Problem Solving,…
- 60’s – present: Cognitive computational models like Model Human Processor, ACT-R, EPIC, Soar

Neurosciences

- 1900’s – 60’s: Beginning theories of neural and brain functions (Helmholtz; Broca, Wernicke)
- 50’s – present: Computational models of neurons: Hodgkin-Huxley, BlueBrain Project,…
- 50’s – present: Computational models of subsystems: visual (Barlow, Hubel-Wiesel), memory (Hopfield), consciousness (Crick-Koch),…
Symbolic Logic (“hard” AI)

- 50’s: Turing Test, “Artificial Intelligence” Dartmouth Symposium, General Problem Solver (Newell and Simon)
- 60’s – 80’s: Symbolic/linguistic focus, expert systems, logic programming, planning and scheduling
- 80’s – present: Cognitive models with a logic bent (eg, Soar)

Computational Intelligence (“soft” AI)

- 40’s: Artificial Neural Networks (ANNs)
- 50’s: ANNs with Learning (Turing again, Hinton, LeCun)
- 60’s – present: Genetic/Evolutionary Algorithms (Holland, Fogel)
- 60’s – 90’s: Fuzzy Logic (Zadeh)
- 80’s – present: Deep Learning. Hinton quote:
  - We’ve ceased to be the lunatic fringe. We’re now the lunatic core.
  - Merging architectures for Big Data and Deep Learning, to influence cognitive architectures