Trends in Large Scale Systems-of-Systems Exemplified by Multi-National Missile Defense

Tod Schuck, PhD
Lockheed Martin RMS
Moorestown, NJ
tod.m.schuck@lmco.com

Jim Kilian, PhD
Lockheed Martin RMS
Burlington, MA
james.c.kilian@lmco.com

LOCKHEED MARTIN

July 2018

Outline

- What do we mean by Large Scale SoS?
  - Multi-Domain
  - Disaggregated; Large numbers of elements; Self-synchronized
  - Large length scale with small to large time scales
  - From physical to cyber-physical to cyber-social systems
  - Multi-National Missile Defense Systems: A motivating example
- Four emerging or evolving areas of interest
  - Variable Autonomy and Human "near-the-loop" variations
    - Artificial and Computational Intelligence
  - Network Resiliency
    - Network analytics and vulnerabilities
    - Network optional vs network assured strategies
  - Institutions in cyber-social systems
    - Principal-Agent Problems
    - Reasoning about commitments
  - Pareto Optimal Design
    - Portfolio analysis and Epoch-Era analyses
- Conclusions

1. Kilian, J., and Schuck, T., "Architecture and Systems-of-Systems Design for Integrated Missile Defense", *2016 11th System of Systems Engineering Conference*, IEEE Conference Publications, Pages: 1 - 6, DOI: 10.1109/SYSOSE.2016.7542913.
2. Schuck, T., and Kilian, J., "Trends in Large Scale Systems-of-Systems for Multi-National Missile Defense", *2017 12th System of Systems Engineering Conference (SoSE),* IEEE Conference Publications. DOI: 10.1109/SYSOSE.2017.7994945

A Few Examples of Large Scale SoS

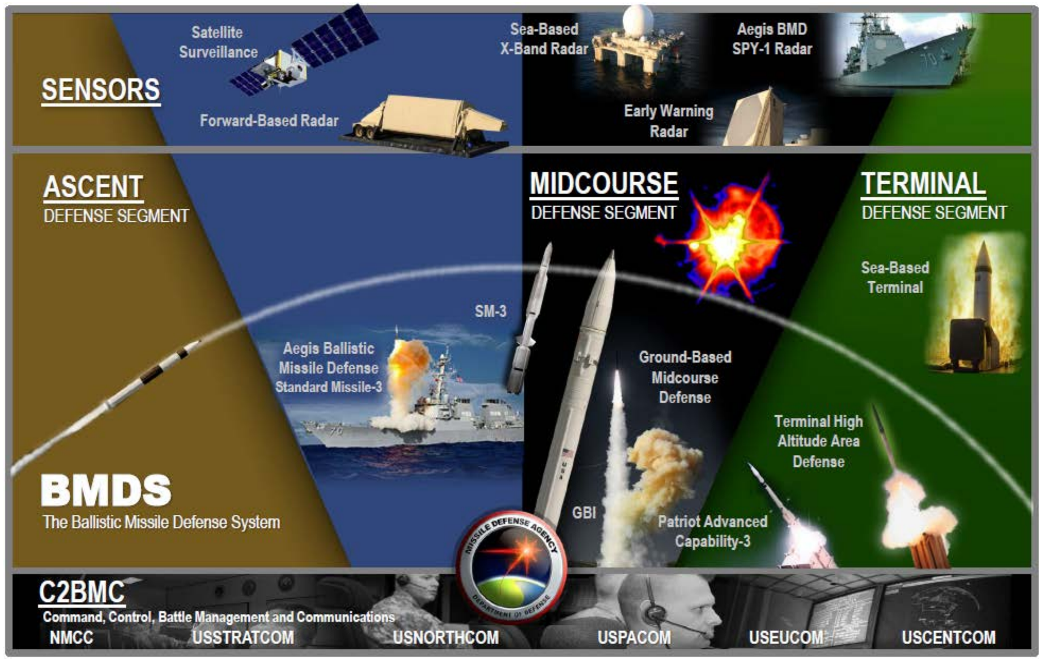
- There is a wide variety of SoS in terms of their purpose, domain of application, complexity, size, novelty, adaptability, quantities, locations, life spans and evolution

- Examples Include
  - Healthcare Management
  - Traffic Management (ports, airports, city, etc)
  - Fleet Maintenance (Predictive maintenance)
  - Home Management (O.K., this one might be small scale)

- Recent areas of interest
  - ULSS: Ultra-large-scale systems are interdependent webs of software, people, policies, and economics – so a software-oriented SoS viewpoint
  - IoT-Driven SoS
  - Autonomous vehicles
  - Enterprise Systems & Architectures

Motivating Application

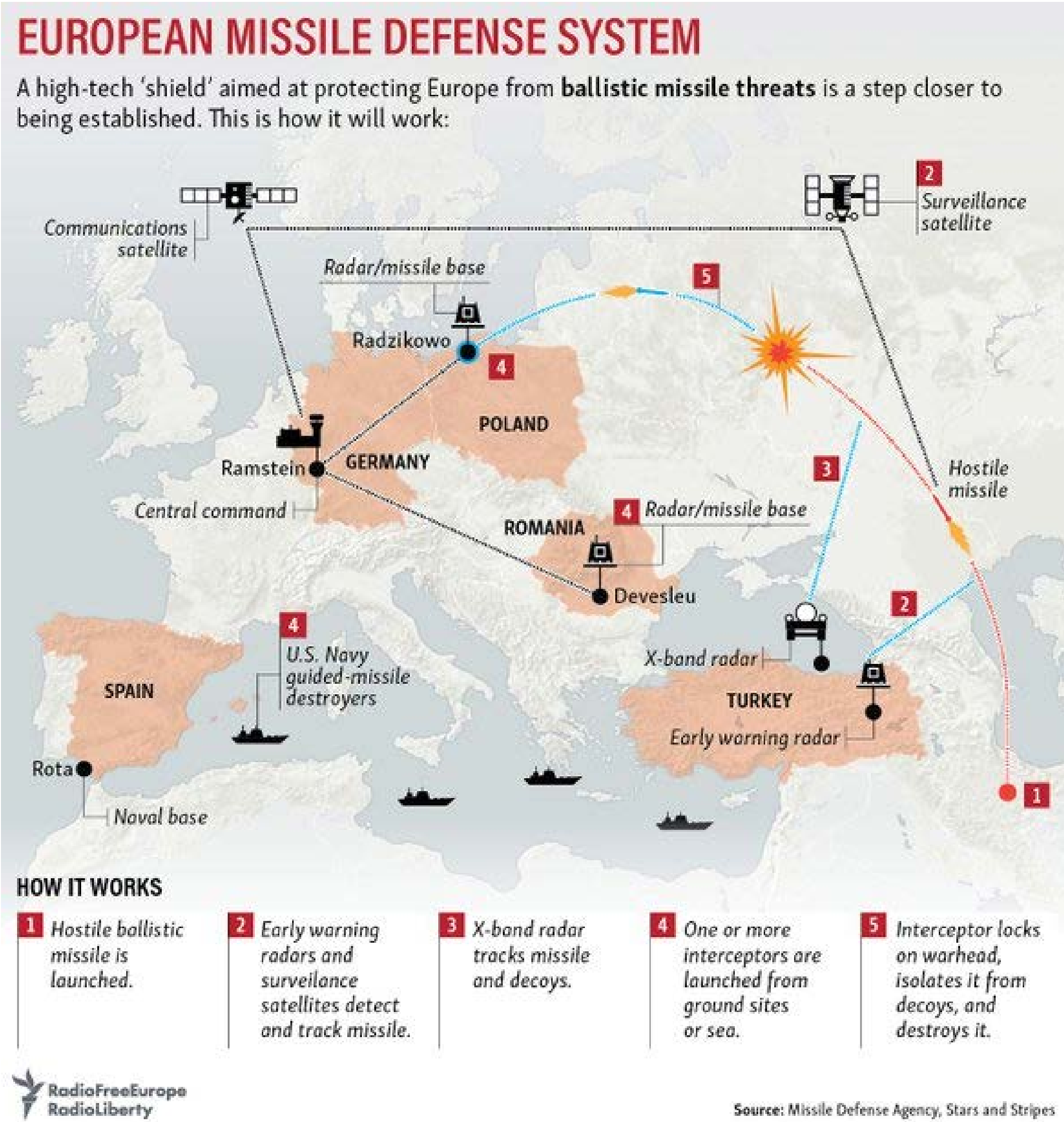
Motivating Application: BMDS



- **The Ballistic Missile Defense System (BMDS) functional concept embodies an integrated, “layered” approach to defense intended to provide multiple opportunities to destroy missiles before they can reach their targets.**
- **The elements of the BMDS**
  - **Networked sensors (including ground, air, sea and space-based sensors)**
  - **Ground- and sea-based interceptor missiles for destroying a threat missile**
  - **A command, control, battle management, and communications (C2BMC) network providing the operational commanders with the needed links between BMDS elements**
- **Missile defense elements are operated by several regional commands from the United States military along with cooperative programs with a number of allies**

MDA, The Ballistic Missile Defense System, http://www.mda.mil/system/system.html .

A Current View – EPAA



What will it take to make all of this work???

SoS Characteristics of Integrated Missile Defense

- **Operational independence – other than potentially at the Combatant Command (COCOM) level, the constituent systems operate under separate command authority using unique interfaces, etc.**
- **Managerial independence – MDA, Navy, Army, Air Force, international partners, etc., separately own all phases for the acquisition process/path for their respective constituent systems with international systems adding another layer of independence**
- **Geographic distribution – Concept of Operations (CONOPS) scenarios guarantee global distribution of constituent systems and multiple interfaces with the systems of international partners**
- **Emergent behavior – this is the direct result of synergy among constituent systems, interaction of these systems with their surroundings**
- **Evolutionary and adaptive development – deployment versions, capabilities, timeframes, etc., are independent (as are the levels of testing and maturity for each system [DOT&E report, 2011])**

Jamshidi, M., ed., *Systems of Systems Engineering, Innovations for the 21st Century*, Wiley , 2009

SoS Typology

Virtual. Virtual SoS lack a central management authority and a centrally agreed upon purpose for the system-of-systems. Large-scale behavior emerges—and may be desirable—but this type of SoS must rely upon relatively invisible mechanisms to maintain it.

BMDSoS Combined Operations

Collaborative. In collaborative SoS the component systems interact more or less voluntarily to fulfill agreed upon central purposes. The Internet is a collaborative system. The Internet Engineering Task Force works out standards but has no power to enforce them. The central players collectively decide how to provide or deny service, thereby providing some means of enforcing and maintaining standards.

BMDSoS Joint Operations

Acknowledged. Acknowledged SoS have recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, and development and sustainment approaches. Changes in the systems are based on collaboration between the SoS and the system.

Directed. Directed SoS are those in which the integrated system-of-systems is built and managed to fulfill specific purposes. It is centrally managed during long-term operation to continue to fulfill those purposes as well as any new ones the system owners might wish to address. The component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose.

The BMD SoS is not contained within a single SoS type

Dahmann, J.S., and K.J. Baldwin, Understanding the current state of US defense systems-of-systems and implications for systems engineering, *IEEE International Systems Conference*, April 2008

Drivers of MNMD SoS Evolution
(and so perhaps of other Large SoS)

Operation in Degraded or Contested Environments

- **Degraded or contested environments result in reduced "–ilities" of the systems of an SoS: Reliability, availability, maintainability**
- **These conditions thereby impose external challenges on realizing emergent properties of SoS**
- **Examples include deception and denial conditions that negate portions of an SoS and/or prevent self-synchronization**

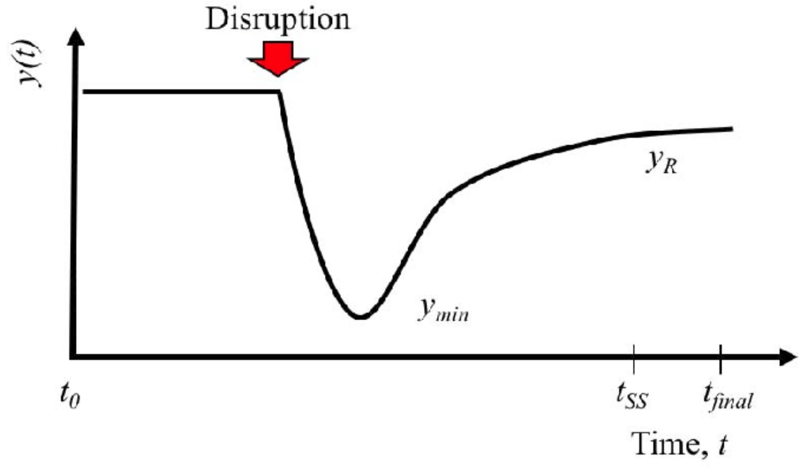
Effective Human-Machine Teaming

- **In the current view of SoS, human elements aren't just external to any system, but part of those systems – cyber-physical-social systems**
- **Human incorporation into SoS design and analysis is further influenced by the types and degrees of autonomy (automation) employed**
  - **Human-in-the-loop**
  - **Human-on-the-loop (must move more towards this…)**
  - **Human-out-of-the loop**
- **Ethical Applications of Autonomy include Meaningful Human Control for example in the sequence for defining, selecting and engaging a target by a weapon**
  - **2400 AI researchers recently signed a pledge to block lethal autonomous weapons**
  - **Much emerging work in "trust in AI"**

Dynamic Command Structures

- Command as the authority vested in an individual, or group, for the direction, coordination and control of military forces is a foundational institution within military organizations
- Multi-national operations are conducted by forces of two or more nations organized as an alliance, a coalition, or other structure, each of which induces yet another institution to define the roles and relationships that in essence define the alliance or coalition
- While the Command institution prevails even in multi-national operations, the recognition of vested command authority expands to include concepts like integrated, lead nation, or parallel command authority
- Thus, a SoS under one or more Command authorities inherits and expresses, through the interactions among its constituents, the institutions that govern multi-national operations, which at times may be in conflict with each other

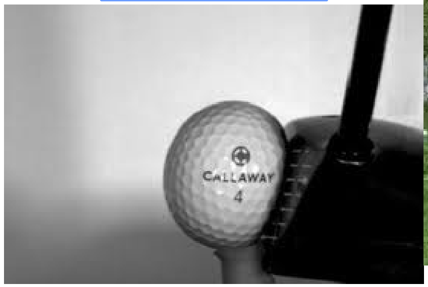
Technology Trends:
Network Resiliency



Resilience vs Robustness

- **The difference:**
  - ***A system is robust when it can continue functioning in the presence of internal and external challenges without fundamental changes to the original system***
  - ***A system is resilient when it can adapt to internal and external challenges by changing its method of operations while continuing to function***
- **Need resilience more than robustness**
  - **Shipboard combat system baselines are designed around redundancy requirements; however, the real systems requirement is based on availability (Ao) – so redundancy has historically been the solution space for this problem, not the design need**
  - **The evolution in high availability complex systems design is moving to the design of resiliency due to the impossibility of anticipating all failure and casualty modes**
- **Resilience in Command and Control (C2) may be achieved, in part, by embracing the paradigm of centralized command, distributed control and distributed execution – also referred to as distributed lethality**
- **However, resilient systems will operate *beyond their designed limits of adaptability***

Resilient



Robust

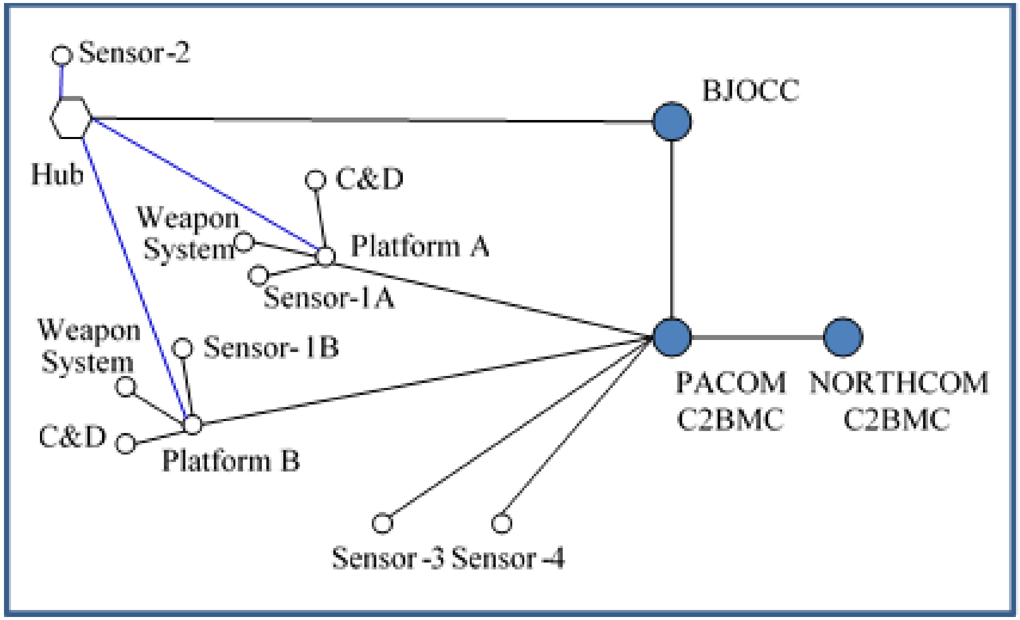
Socio-Dynamic Networks

- **Four tenets of Network-Centric Operations (Network Enabled Capability in NATO) consist of:**
  - **A robustly networked force improves information sharing**
  - **Information sharing and collaboration enhance the quality of shared situational awareness (Single Integrated Cross-Domain Picture)**
  - **Shared situational awareness enables self-synchronization**
  - **Enhanced shared situational awareness and self-synchronization increases mission effectiveness**
- **Starting with work in neurobiology, we note there are three types of connectivity which can be explored in network systems:**
  - **Structural connectivity – physical connection between nodes**
  - **Functional connectivity – temporal correlations between nodes**
  - **Effective connectivity – a causal connection between nodes**

Socio-Dynamic Networks

- **Structural: The connective fabric hosting the structural network, referred to previously as an instantiation of an MNMDS, is a reflection of the global information grid (GIG) architecture that drives the transformation of military operations to net-centric operations and expressed in a missile defense context - the implication is that all nodes in the network can potentially be connected to all other nodes via a realized GIG**
- **Functional: Often expressed in terms of flows on a physical network where each functional activation pattern is identified as its own network, thus we may have a Planning Functional Network, a Search Functional Network, a Tracking Functional Network, a Discrimination Functional Network, and a Fire Control Functional Network**
- **Effective: We consider the properties, shared and otherwise, of these Functional Networks along with attributes imposed on shaping the underlying Structural Network that is the physical SoS**

Socio-Dynamic Networks

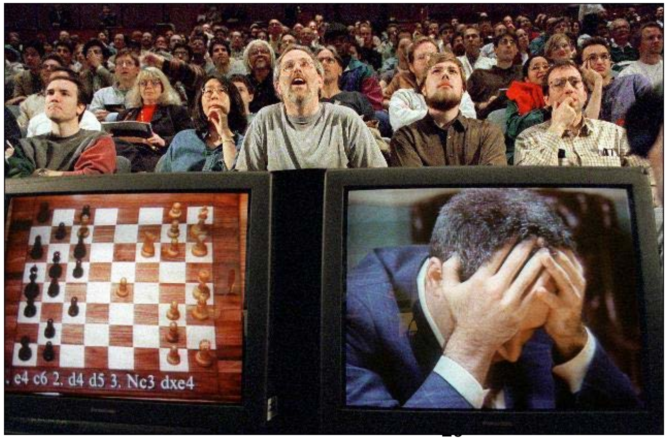


- **Network and functional motifs look for patterns of local structural connectivity**
  - **Path lengths, information specialization, clustering, connectivity, integration, etc.**
- **Measures of centrality measure a node's connective importance, it's ability to facilitate integration and its role in resilience of the network to attack**

Technology Trends:
Variable Autonomy and Human "Near-the-Loop" Variations

Integrated Human-Machine Teaming

- **In 2005, two amateur chess players using three personal computers won a chess tournament against a field consisting of both supercomputers and (human) grandmasters**
- **Gary Kasparov dubbed this mode of play as “Centaur Chess”, because the human chess-players (the head) used chess software (the body) as an advisor – the human making the final decision about the move to take**
- **This sort of human-machine teaming (HMT) for combat is one of the building blocks envisioned in the Third Offset Strategy from the Department of Defense and so constitutes a focused area of investment for technology and system research and development**
- **A current HMT example is the coupling of (manned) AH-64 Apache helicopters together with Grey Eagle UAV operating as remotely controlled extensions of the manned system’s onboard sensors – with such a team, Apaches and Shadow UAVs, recently returned from a deployment in Iraq**



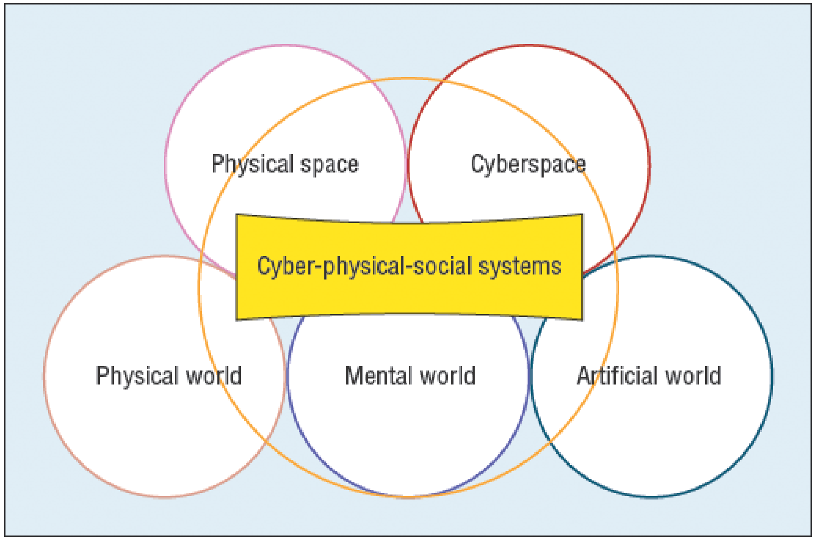
Computational Intelligence

- Alberts et al. describe the concept of four “domains” of C2 in several works which include the Physical, Information, Cognitive, and Social
- Specifically, the Cognitive Domain is where “perceptions, awareness, beliefs, and values reside and where, as a result of sense-making, decisions are made”
- The Social Domain is where “interactions between and among force entities occurs”
- Citing work done by the SAS-050 NATO Working Group, Alberts et al. relate that data in context becomes information
  - Information becomes awareness when it is sorted in the human brain
  - Situation understanding (or awareness (SA)) occurs when prior knowledge and mental models are employed
  - Shared information, awareness, and understanding can now occur across nodes – this in turn drives decision-making and enables CI

Computational Intelligence

- **Increasingly, the speed of the threat space across both existing and new warfare areas is necessitating the use of more automated methods for processing information and making decisions**
  - **DARPA Target Recognition and Adaptation in Contested Environments (TRACE) program (AI and fusion) and DL are examples**
- **The human brain cannot keep up with the speed of information in a modern contested environment – example, 80-85% of institutional trades in the NYSE are done via high-speed algorithmic methods**
- **Llinas and Rogova describe an approach as a "data fusion-based human-machine threat recognition approach that combines story-based augmentation and the Transferable Belief Model (TBM) for belief management, decision fusion, and anytime decision-making"**
- **Schuck and Blasch describe a knowledge representation method using the Choquet Integral and a Bayes risk method to determine the intent and to predict the future action of an adversary**

Technology Trends:
Institutions in cyber-social systems



Institutions

- **Behavioral norms in organizations can be viewed as constraints (the regimented view) or as explicit expression and enforcement of commitments through institutions (regulated view)**
- **Institutions are coordination artifacts that constitute the interface between internal agent capabilities and the social effect of their interactions**
- **Agent organizations must consider not only individual goals and capabilities, but such organizational characteristics as stability, predictability and commitment to aims and strategies**
- **Institutions then are either first-class entities, agents in their own right, in a MAS, or they are the (possibly dynamic) rules of a game between the agents in a MAS**

Commitments

- **Given a pair of agents x and y, along with propositions G (preconditions) and p (post-conditions), then a *(social) commitment* from x to y is an expression, $C_{x,y}(G, p(x))$, that states if G holds, then x will bring about p**
  - **Example: Seller agrees to send the book, *Multi-Agent Systems*, to Buyer, if Buyer pays Seller $20**

    $$[\ C_{S,B}(pay\$20(B) \wedge HasBook(S),\ SendBook(S))\ ]$$
- **Commitment States**
  - **Holds/¬Holds**
  - **Detached:** $C_{x,y}(\top, p(x))$
  - **Discharged:** $C_{x,y}(G, \top)$
- **Operations on Commitments include**
  - **Create(C) : x establishes a commitment to y**
  - **Cancel(C) : x nullifies its commitment to y**
  - **Release(C) : y releases x its commitment**
  - **Delegate(C) : x transfers the commitment to z:**

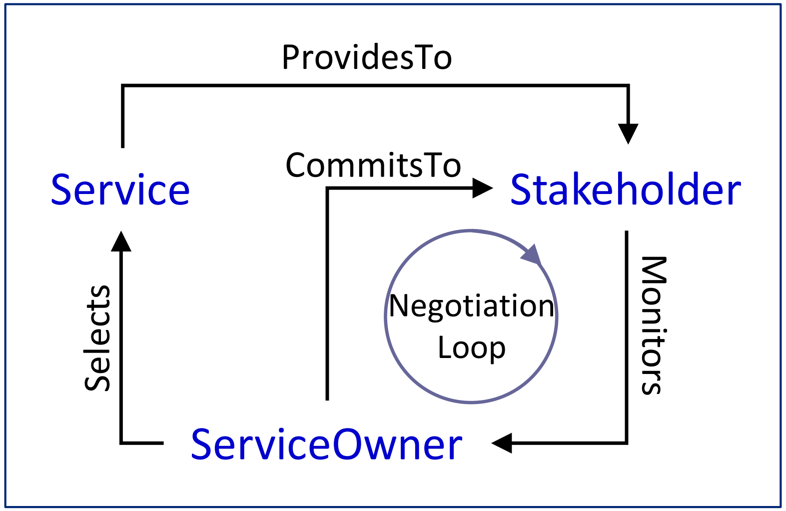
    $$C_{x,y}(G_{x,y}, p(x)) \rightarrow C_{z,y}(G_{z,y}, p(z))$$
  - **Assign(C) : y transfers its obligation to w:** $C_{x,y}(G_{x,y}, p(x)) \rightarrow C_{x,w}(G_{x,w}, p(x))$

More Institutions

- An institution behind the book buying commitment: A Marketplace
  – Establishes the rules governing participation – there is the ubiquitous user agreement (that everyone signs and no-one reads)
  – Monitors participant behavior
  – Applies incentives for correct behavior and penalties for incorrect behavior from participants
  – Acts as a broker
- Other institutions that govern interactions in MAS
  – Voting systems
  – Taxation systems
  – Bribery systems
  – Insurance systems
  – Legal systems
  – Auctions/Reverse Auctions
  – Contracting systems
- Multiple institutions may be in play for a BMDMAS
  – Multi-Attribute Reverse Auction as a protocol to establish *Contracts*
  – Treaty institutions that host Contracting Systems

Reasoning About Commitments

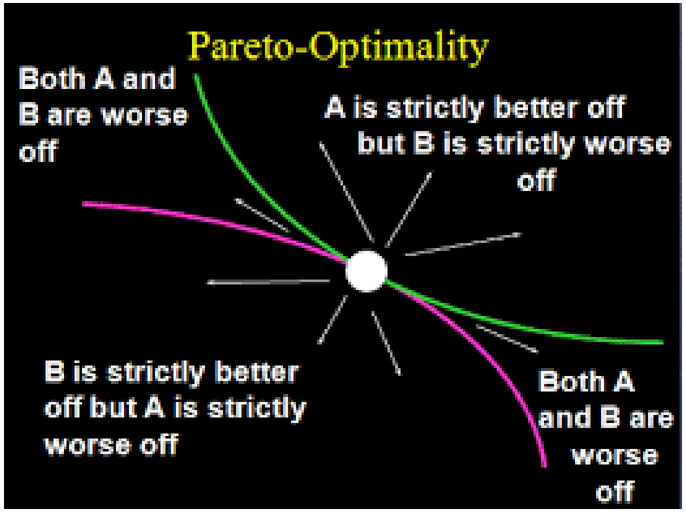
- **An Institution as an autonomous (or partially autonomous) agent in a MAS, may need the ability to represent and reason about commitments**
- **Recently an approach to representing commitments, in the context of MNMDS, was described utilizing a temporal deontic logic [14]**
- **Deontic logic is a first order modal logic which has modal operators for _obligation_ and _permission_**
- **Conflicting obligations arising from a preference ordering can be represented in this formalism**



Abstract elements of an SoS

Self-Defense ≥ Homeland Defense ≥ Defended Area ≥ Coalition Defense

Technology Trends:
Pareto Optimality



Growing Complexity of SoS

- **There are three "tiers" of design abstraction:**
  - **System-Level: From Walton, system design occurs at a "level of decomposition that is inclusive of a major architectural element and is semi-independent from the rest of the architecture"**
    - **The designer of a system typically has full design authority, and although a system may be composed of multiple components (such as a launch vehicle) it is not considered a SoS as the sub-elements are not managerially independent**
  - **Program-Level: Program design is distinguished from system design in that it requires joint consideration of multiple independent or semi-independent constituent elements (typically systems themselves)**
    - **However, like system-level analysis, the designer of a program is typically assumed to have a moderate to high degree of design authority**
    - **Two primary types of programs have been identified (homogeneous and heterogeneous), and they are distinguished by the attributes of the constituent systems**
  - **Portfolio-Level: A portfolio is a collection of selected assets that may be either new or legacy programs as defined above, which are simultaneously invested in to collectively provide a set of capabilities**
    - **A portfolio designer does not necessarily have a significant level of control over the design of the constituent programs, or their ultimate operationalization in a SoS, but can create a portfolio with attractive procurement, management, and capability features based upon the possible assets and their likely applications**

Epoch-Era Analysis

- **The evolution of Tradespace Exploration (TSE) as a means for achieving Engineered Resilient Systems has as its most recent expression work out of the Systems Engineering Advancement Research Initiative (SEAri) at MIT in the form of Epoch-Era Analysis.**
- **The Tradespace is the space spanned by the completely enumerated design variables, which means given a set of design variables, the tradespace is the space of possible design options.**
- **In TSE, utility versus cost is plotted for variations in the design variables.**
- **The goal is to locate the configurations that lie on the Pareto Frontier. Epoch-Era Analysis (EEA) extends TSE by building in dynamics arising from changes to the system/context/needs.**
- **In EEA epochs are periods of fixed context and needs (short run). Eras are sequences of epochs simulating a potential future lifecycle path experienced by the system (long run).**
- **TSE tends to focus on system alternatives within a static context and needs. EEA explicitly considers the dynamic environment in which the system will need to sustain value delivery to its stakeholders.**

Conclusions

- The engineered MNMDS is not a simple system of loose confederates that somehow work together in an optimal fashion – a true SoS approach must be undertaken in order to have success across multi-national domains that span technical, operational, and command elements
  - First, deliberate work must occur in ERS as part of the concept realization for distributed lethality and MDS
  - Second, HMT is the next evolution of human and technology integration/collaboration that is required in order for massive amounts of data and information to be used to create knowledge states for humans to be able to apply effectively for decision-making
  - Third, principal-agent problems need to be solved so that a regional MNMDS will work
- For all of this, the *collective response* of a SoS is critical – understanding that a MNMDS is described by the five conditional properties of operational & managerial independence, geographic distribution, emergent behavior, and evolutionary/adaptive characteristics
- Socio-Dynamic networks allow us to consider the property of shared awareness within varying levels of connectivity for a MNMDS
- Automated SA is desired for advanced threat understanding to relieve the human who is in or on the decision-making loop from data overload – we propose the use of *computational awareness* initiatives to enable *tacit awareness* in a processing enterprise to enable threat reaction and overall SoS optimization

Sources (complete list in IEEE papers)

[1] D.S. Alberts and R.E. Hayes, *Understanding Command and Control*, Department of Defense Command and Control Research Program (CCRP) Publication Series, 2006.

[2] D.S. Alberts, J.J. Garstka, R.E. Hayes, and D.A. Signori, *Understanding Information Age Warfare*, Department of Defense Command and Control Research Program (CCRP) Publication Series, August 2001.

[3] D.S. Alberts and R.E. Hayes, *Power to the Edge, Command, Control, in the Information Age*, Department of Defense Command and Control Research Program (CCRP) Publication Series, April 2005.

[4] K. Allard, Command, Control and the Common Defense, National Defense University, Institute for National Strategic Studies, revised, 1996.

[5] D.S. Bassett and E. Bullmore, "Small-World Brain Networks", *Neuroscientist*, 12(6), 512–523, 2006.

[6] S. Braynov and T. Sandholm, "Contracting with Uncertain Level of Trust", Computational Intelligence, Vol. 18, No. 4, 501-514, 2002.Chairman Joint Chiefs of Staff, U.S. Dept. of Defense, Multi-National Operations, Joint Publication 3-16, July 16, 2013.

[7] D. Brutzman, *Network Optional Warfare (NOW) Operational Concepts and Enabling Technologies*, Presentation from the Undersea Warfare Group, Information Sciences Department, Naval Postgraduate School, March 2, 2014.

[8] K. de Angelis and J. Garfield, "Give Commanders the Authority", *US Naval Institute Proceedings Magazine*, Vol. 142, No. 10, 1364, October 2016.

[9] M. DiMario, J. Boardman, J. Sauser, System of Systems Collaborative Formation, IEEE Systems Journal, 3(3), 360-368, 2009

[10] D. Destito, and T. Schuck, "BMD Capabilities at all Levels of Conflict", National Fire Control Symposium, Nellis AFB, Nevada, 2012.

[11] J. Drew, "First Shadow-Apache MUM-T Unit Returns from Iraq", *Aerospace Daily & Defense Report*, June 7, 2016.

[12] S.J. Freedberg Jr., "Centaur Army: Bob Work, Robotics and the Third Offset Strategy", *Breaking Defense*, Nov. 09, 2015.

[13] R.K. Garrett, Jr., S. Anderson, N.T. Baron, and J.D. Moreland, Jr., Managing the Interstitials: A System of Systems Framework Suited for the Ballistic Missile Defense System, *Systems Engineering*, 14(1), 2010.

[14] T.J. Grant, Formalized Ontology for Representing C2 Systems as Layered Networks, ", Ch. 5 in *Network Topology in Command and Control*, p. 85-124, (IGI Global), 2014.

Sources (complete list in IEEE papers)

[15] G.M. Hostage III, Gen. USAF and L.R. Broadwell Jr., LTC USAF, "Resilient Command and Control, The Need for Distributed Control", *Joint Force Quarterly*, Vol. 74, 38-43, 2014.

[16] M. Jamshidi,"Introduction to System of Systems", *Systems of Systems Engineering, Innovations for the 21st Century*, John Wiley and Sons Inc., 2009

[17] J. Kilian and T. Schuck, "Architecture and System-of-Systems Design for Integrated Missile Defense", IEEE 11th Systems of Systems Engineering Conference, 2016.

[18] J. Kline, "A Tactical Doctrine for Distributed Lethality", Center for International Maritime Security, 22 February 2016.

[19] M.W. Maier, "Architecting Principles for Systems-of-Systems", *Systems Engineering*, Vol 1, No. 4, pp. 267-284, 1998.

[20] Office of the Director, *Operational Test and Evaluation (DOT&E) FY 2011 Annual Report* December, 2011, pp. 251-254.

[21] T. Rowden, P. Gumataotao, and P. Fanta, "Distributed Lethality", *US Naval Institute Proceedings Magazine*, Vol. 141, No. 1, 1343, January 2015.

[22] T.M. Schuck and E. Blasch, "Description of the Choquet Integral for Tactical Knowledge Representation", *IEEE 13th Annual Conference on Information Fusion*, July 2010.

[23] Schuck, T.M. and J.C. Kilian, "Trends in Large-Scale Systems-of-Systems for Multi-National Missile Defense", IEEE 12th Systems of Systems Engineering Conference, 2017.

[24] A.B. Urken, A. Nimz and T.M. Schuck, Designing Evolvable Systems in a Framework of Robust, Resilient and Sustainable Engineering Analysis, *Advanced Engineering Informatics*, 26, 553-562, 2012.

[25] M.A. Walton, *Managing Uncertainty in Space Systems Conceptual Design Using Portfolio Theory*, PhD Dissertation, MIT Dept. Aeronautics/Astronautics, 2002.

[26] G. Warwick and J. D. Washington, "Targeted Learning", *Aviation Week and Space Technology*, 45-46, June 6-19, 2016.

[27] M.S. Wu, A.M. Ross and D.H. Rhodes, "Design for Affordability in Complex Systems and Programs Using Tradespace-based Affordability Analysis", *Conference on Systems Engineering Research* (CSER 2014), pp 828-837, 2014.

[28] S. Yang, "Emerging Behavior of Financial Market", Stevens Institute of Technology -Accenture ACE Workshop, Hoboken, NJ, 2015.