PROCEEDINGS OF SPIE

Signal Processing, Sensor/Information Fusion, and Target Recognition XXIII

Ivan Kadar
Editor

5–8 May 2014
Baltimore, Maryland, United States

Sponsored and Published by
SPIE

Volume 9091

Proceedings of SPIE 0277-786-786X, V.9091

SPIE is an international society advancing an interdisciplinary approach to the science and application of light.

Signal Processing, Sensor/Information Fusion, and Target Recognition XXIII, edited by Ivan Kadar, Proc. of SPIE
Vol. 9091, 909101 · © 2014 SPIE · CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2072534

Please use the following format to cite material from this book:
Author(s), "Title of Paper," in *Signal Processing, Sensor/Information Fusion, and Target Recognition XXIII*, edited by Ivan Kadar, Proceedings of SPIE Vol. 9091 (SPIE, Bellingham, WA, 2014) Article CID Number.

ISSN: 0277-786X
ISBN: 9781628410280

Published by
SPIE
P.O. Box 10, Bellingham, Washington 98227-0010 USA
Telephone +1 360 676 3290 (Pacific Time)· Fax +1 360 647 1445
SPIE.org

Printed in the United States of America.

Publication of record for individual papers is online in the SPIE Digital Library.

SPIEDigitalLibrary.org

Paper Numbering: Proceedings of SPIE follow an e-First publication model, with papers published first online and then in print and on CD-ROM. Papers are published as they are submitted and meet publication criteria. A unique, consistent, permanent citation identifier (CID) number is assigned to each article at the time of the first publication. Utilization of CIDs allows articles to be fully citable as soon as they are published online, and connects the same identifier to all online, print, and electronic versions of the publication. SPIE uses a six-digit CID article numbering system in which:

- The first four digits correspond to the SPIE volume number.
- The last two digits indicate publication order within the volume using a Base 36 numbering system employing both numerals and letters. These two-number sets start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B … 0Z, followed by 10-1Z, 20-2Z, etc.

The CID Number appears on each page of the manuscript. The complete citation is used on the first page, and an abbreviated version on subsequent pages. Numbers in the index correspond to the last two digits of the six-digit CID Number.

Contents

POSTER SESSION

Conference Committee

Symposium Chair

David A. Whelan, Boeing Defense, Space, and Security (United States)

Symposium Co-chair

Nils R. Sandell Jr., Strategic Technology Office, DARPA (United States)

Conference Chair

Ivan Kadar, Interlink Systems Sciences, Inc. (United States)

Conference Co-chairs

Erik P. Blasch, Air Force Research Laboratory (United States)
Kenneth Hintz, George Mason University (United States)
Thia Kirubarajan, McMaster University (Canada)
Ronald P. S. Mahler, Lockheed Martin Corporation (United States)

Conference Program Committee

Mark G. Alford, Air Force Research Laboratory (United States)
William D. Blair, Georgia Tech Research Institute (United States)
Mark J. Carlotto, General Dynamics Advanced Information Systems (United States)
Kuo-Chu Chang, George Mason University (United States)
Chee-Yee Chong, Independent Consultant (United States)
Marvin N. Cohen, Georgia Tech Research Institute (United States)
Frederick E. Daum, Raytheon Company (United States)
Mohammad Farooq, AA Scientific Consultants Inc (Canada)
Charles W. Glover, Oak Ridge National Laboratory (United States)
I. R. Goodman, Consultant (United States)
Lynne L. Grewe, California State University, East Bay (United States)
David L. Hall, The Pennsylvania State University (United States)
Michael L. Hinman, Air Force Research Laboratory (United States)
Jon S. Jones, Air Force Research Laboratory (United States)
Martin E. Liggins II, Consultant (United States)
James Llinas, University at Buffalo (United States)
Raj P. Malhotra, Air Force Research Laboratory (United States)
Alastair D. McAulay, Lehigh University (United States)
Raman K. Mehra, Scientific Systems Company, Inc. (United States)
Harley R. Myler, Lamar University (United States)

David Nicholson, BAE Systems (United Kingdom)
Les Novak, Scientific Systems Company, Inc. (United States)
John J. Salerno Jr., Air Force Research Laboratory (United States)
Andrew G. Tescher, AGT Associates (United States)
Stelios C. A. Thomopoulos, National Center for Scientific Research Demokritos (Greece)
Wiley E. Thompson, New Mexico State University (United States)
Pierre Valin, Defence Research and Development Canada, Valcartier (Canada)

Session Chairs

1 Multisensor Fusion, Multitarget Tracking, and Resource Management I
Ivan Kadar, Interlink Systems Sciences, Inc. (United States)
Kenneth Hintz, George Mason University (United States)

2 Multisensor Fusion, Multitarget Tracking, and Resource Management II
Kenneth Hintz, George Mason University (United States)
Ivan Kadar, Interlink Systems Sciences, Inc. (United States)
Thia Kirubarajan, McMaster University (Canada)

3 Information Fusion Methodologies and Applications I
Ronald P. Mahler, Lockheed Martin Corporation (United States)

4 Information Fusion Methodologies and Applications II
Michael L. Hinman, Air Force Research Laboratory (United States)
Ivan Kadar, Interlink Systems Sciences, Inc. (United States)

5 Information Fusion Methodologies and Applications III
Michael L. Hinman, Air Force Research Laboratory (United States)
Kenneth Hintz, George Mason University (United States)
Ivan Kadar, Interlink Systems Sciences, Inc. (United States)

6 Information Fusion Methodologies and Applications IV
Erik P. Blasch, Air Force Research Laboratory (United States)
Michael L. Hinman, Air Force Research Laboratory (United States)
Kenneth Hintz, George Mason University (United States)
Ivan Kadar, Interlink Systems Sciences, Inc. (United States)

7 Signal and Image Processing, and Information Fusion Applications I
Lynne L. Grewe, California State University, East Bay (United States)
Mark J. Carlotto, General Dynamics Advanced Information Systems (United States)

8 Signal and Image Processing, and Information Fusion Applications II
Mark J. Carlotto, General Dynamics Advanced Information Systems (United States)
Lynne L. Grewe, California State University, East Bay (United States)

9 Signal and Image Processing, and Information Fusion Applications III
Mark G. Alford, Air Force Research Laboratory (United States)
Mark J. Carlotto, General Dynamics Advanced Information Systems (United States)
Lynne L. Grewe, California State University, East Bay (United States)

10 Signal and Image Processing, and Information Fusion Applications IV
Mark G. Alford, Air Force Research Laboratory (United States)
Mark J. Carlotto, General Dynamics Advanced Information Systems (United States)
Lynne L. Grewe, California State University, East Bay (United States)

11 Signal Processing, Information Fusion, and Understanding Aspects of Cyber Physical Systems
Lynne L. Grewe, California State University, East Bay (United States)

Invited Panel Discussion: Issues and Challenges of Information Fusion in Contested Environments
Erik P. Blasch, *Moderator*, Air Force Research Laboratory (United States)
Ivan Kadar, *Moderator*, Interlink Systems Sciences, Inc. (United States)
Chee-Yee Chong, Independent Consultant (United States)
Laurie H. Fenstermacher, Air Force Research Laboratory (United States)
John D. Gorman, SET Corporation (United States)
Eric K. Jones, Systems & Technology Research (United States)
Georgiy M. Levchuk, Aptima, Inc. (United States)
Jorge E. Tierno, Barnstorm Research Corporation (United States)

Introduction

In contested environments, fusion has to address challenges not present in available environments, such as: objects of interest may be hard to detect due to concealment; sensing may be at stand-off distances and observations may be sparse; communication could be unreliable due to possible jamming; and bandwidth may be limited. Thus information fusion methods have to deal with more difficult targets using a lower quality and quantity of data over less capable communications networks. Similarly, in cyberspace/networking, information transfer may be compromised by malware, malicious attacks or just by phishing or spam potentially affecting both information sources and the efficient use of the sources for analysis and decision making.

The objective of this panel was to bring to the attention of the fusion community the importance of dealing with contested information sources, highlighting issues, illustrating potential approaches and addressing challenges. The panel addressed issues and challenges in contested environments highlighting the problem of acquiring, representing, handling, processing, fusing and using information sources in competitive environments and presented systems-level examples of potential "defensive approaches" (winning strategies in contests). A number of invited experts discussed challenges of the fusion process and research to address these challenges. The panelists illustrated parts of the abovementioned areas over different applications, and addressed applications to all levels of information fusion. Conceptual and real-world related examples associated with the overall complex problem were used by the panel to highlight impending issues and challenges.

Ivan Kadar
Erik Blasch
Chee-Yee Chong

Invited Panel Discussion
Issues and Challenges of Information Fusion in Contested Environments

Organizers

Chee-Yee Chong, Independent Consultant

Erik Blasch, Air Force Research Lab., Rome Research Site.

Ivan Kadar, Interlink Systems Sciences, Inc.

Moderators

Erik Blasch, AFRL

Ivan Kadar, Interlink Systems Sciences, Inc.

May 5, 2014

SPIE Conference 9091

“Signal Processing, Sensor Fusion and Target Recognition XXIII
Baltimore, MD., 5–8 May 2014

Invited Panel Discussion
Panel Participants:

Dr. Erik Blasch, Air Force Research Lab., Rome Research Site, U.S.A.

Dr. Chee-Yee Chong, Independent Consultant, U.S.A.

Dr. Laurie Fenstermacher, Air Force Research Lab., WPAFB, U.S.A.

Dr. John D. Gorman, DARPA, U.S.A

Dr. Eric K. Jones, Systems and Technology Research, U.S.A.

Dr. Ivan Kadar, Interlink Systems Sciences, Inc., U.S.A.

Dr. Georgiy Levchuck, Aptima, Inc.,U.S.A.

Dr. Jorge E. Tierno, Barnstorm Research Corp., U.S.A.

Invited Panel Discussion

Topics

“Perspectives on and Applications of Information Fusion in Contested Environments”
Dr. Ivan Kadar, Interlink Systems Sciences, Inc.

”Fusion in Contested Environments”
Dr. Chee-Yee Chong, Independent Consultant

"Information Fusion Designed for (Robust) Action”
Dr. Jorge E. Tierno, Barnstorm Research Corp.

“Intelligence, Surveillance and Reconnaissancein Contested Environments”
Dr. Eric K. Jones, Systems and Technology Research

Invited Panel Discussion

Topics

”Systems of Systems Distributed ISR”
Dr. John D. Gorman, DARPA

“Information Fusion in Contested Environments”
Dr. Erik Blasch, Air Force Research Lab.

“Open Source Information: Implications for Information Fusion in Contested Environments”
Dr. Laurie Fenstermacher, Air Force Research Lab.

“Autonomy, Heterogeneity, and Collaboration in Contested Environments”
Dr. Georgiy Levchuk, Aptima, Inc.

Perspectives on and Applications of Information Fusion in Contested Environments

Ivan Kadar
Interlink Systems Sciences, Inc.
Lake Success, NY, USA
5 May 2014

Invited Panel Discussion on "Issues and Challenges of Information Fusion in Contested Environments"

SPIE Conference 9091 "Signal Processing, Sensor Fusion and Target Recognition XXIII", 5-8 May 2014, Baltimore, MD

Outline/Motivation

- The purpose of this talk is to highlight constituent elements of "Contested Environments" (CE) which, to various degrees, have always been considered in systems designs and operations, and the role of information fusion.
- The above ushers in several Domains of CEs, subsets of which are used to illustrate **Issues and Challenges**:
  - Methods of "Defense" (Winning Strategies) via a *"systems level approach" to eliminate/reduce the effects of CEs on operational performance incorporating domain specific applications of information fusion

Representative environments (causes and effects) include:

- Electronic Warfare (EW): jamming, deception, spoofing, countermeasures
- Areas-of-Denial: EW or Environment Induced, Stealth, Kinematic attacks
- Information Warfare: Denial-of-Information (DOI) & Denial-of-Service (DOS)
- Deceptions for Exploitation/DOI (spam, malware, phishing) in Cyberspace
- Cyber Warfare (Computer Network Attacks)
- Contested Collaboration in Command-and-Control (C2) & Social Networks

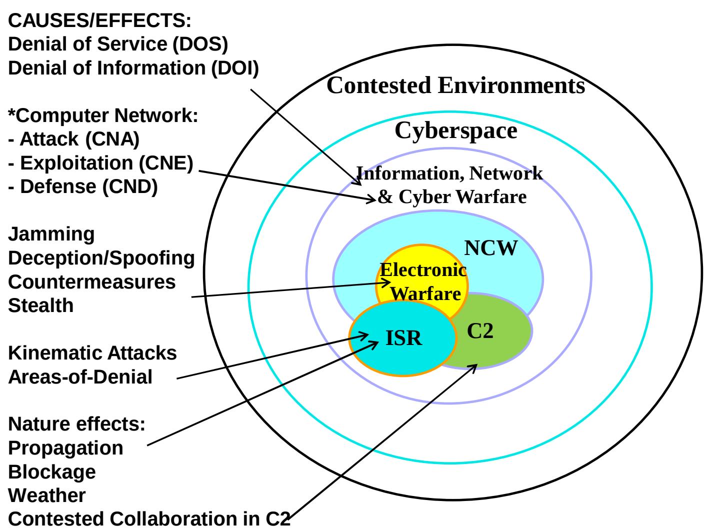
*http://www.darpa.mil/Our_Work/STO/

Outline/Motivation (Cont'd)

Issues and Challenges of Defensive Approaches Addressed:

- A Cyber Information Processing System for DOI Defense and Data Analysis
- Analyst Cognition Modeling in OODA Loop, and its Relationship to user Data Fusion Information Group (DFIG) Model – in Cyber DOI Defense
- Challenges of Contested Collaboration in Human Data Collection for Physics and Human Derived (a.k.a. Hard and Soft) Information Fusion
- Mobile Agents-Based Incremental Data Fusion in Jammed UGS/Wireless Sensor Networks (WSN)
- Peer-to-Peer (P2P) Networks vs. Client Server for NCW/C2/BM/ISR
- Example of a highly successful operational NCW C2/BM/ISR P2P Networked Anti-Jam System in Contested Environments using Measurement Domain Fusion: "Cooperative Engagement Capability (CEC)"; Applications illustrated: Littoral Battle Environment, Principal Functions and Conceptual Ballistic Missile Defense Scenario

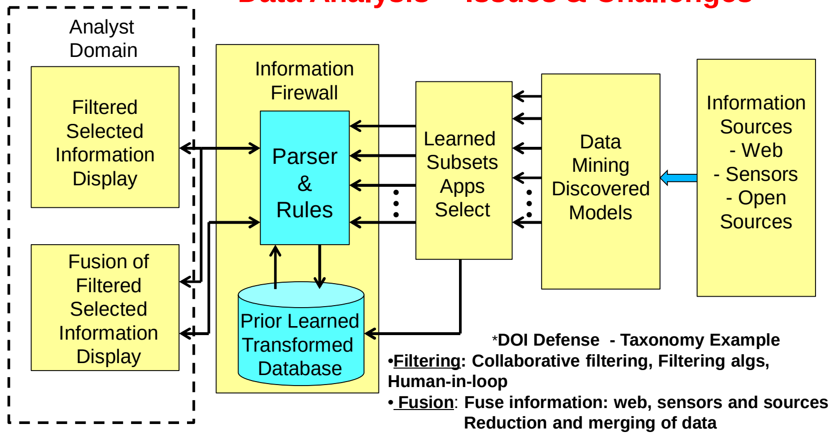
Example: Domains of Contested Environments



Note: Space Borne CE not Addressed

*M. Miller, J. Brickey, and G. Conti, "Why Your Intuition About Cyber Warfare is Probably Wrong", *Small Wars Journal*, 29 Nov 2012.

A Cyber Info Processing System Concept for DOI Defense and Data Analysis - Issues & Challenges

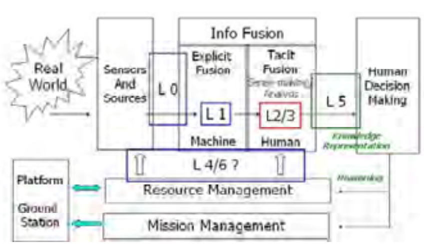


*DOI Defense - Taxonomy Example

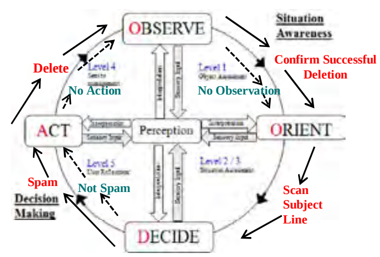
- **Filtering**: Collaborative filtering, Filtering algs, Human-in-loop
- **Fusion**: Fuse information: web, sensors and sources
  Reduction and merging of data
  Enhanced analyst's decision making ability
- **Transform Data:** Converting data into preferred forms

*G. Conti and M. Ahamad; "A Taxonomy and Framework for Countering Denial of Information Attacks" *IEEE Security and Privacy*. November/December 2005.
G. Conti, M. Ahamad and R. Norback; "Filtering, Fusion and Dynamic Information Presentation: Towards a General Information Firewall;" *IEEE International Conference on Intelligence and Security Informatics (IEEE-ISI)*; May 2005. Talk PPT Slides(2.0M))

Representing "Cyber DOI Defense" in the OODA Loop and OODA in Relation to DFIG User Fusion Model



*Data Fusion Information Group (DFIG) Model

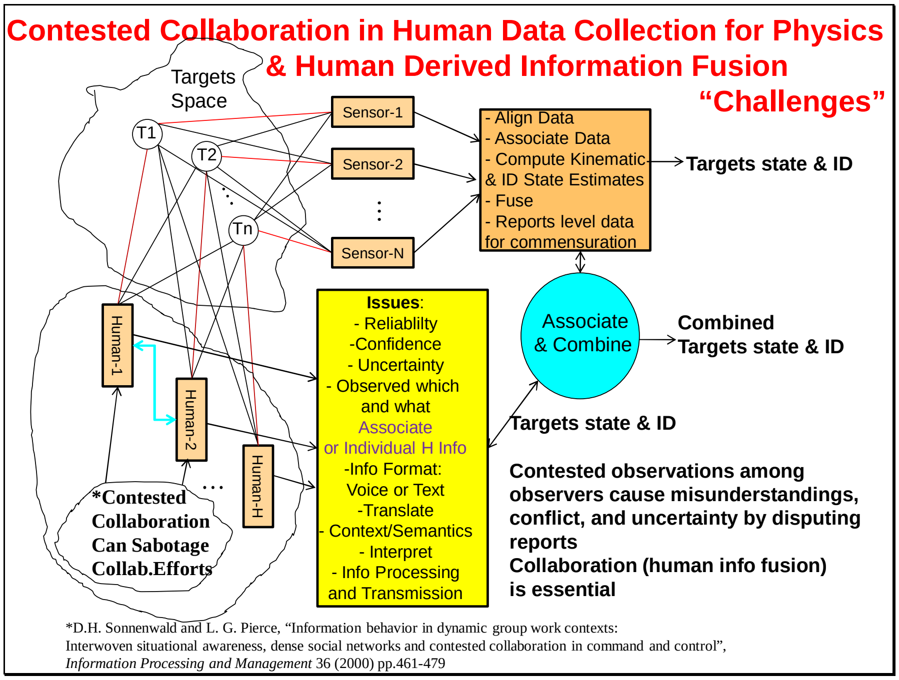


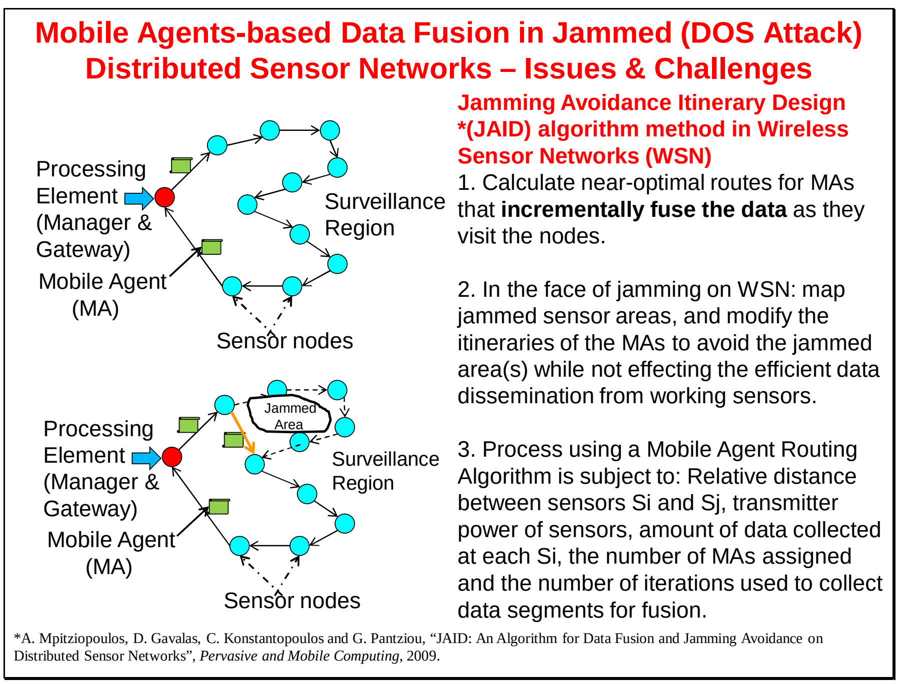
*Observe, Orient, Decide, Act (OODA) Loop in relation to the DFIG model - **OODA in Cyber Attacks defense

- Note: **"Spam" in example can be replaced by "Phishing" or "Malware" in DOI attacks, i.e., Cyberspace in Contested Environment
- Note importance of human operator/analyst cognitive defensive role

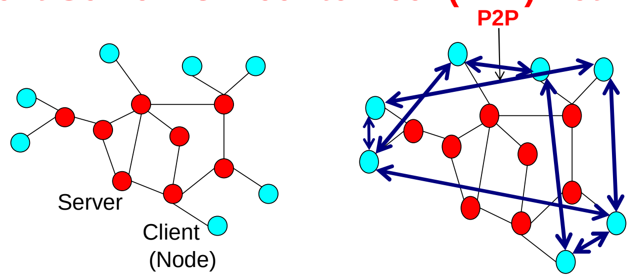
*E. Blasch, R. Brenton, P. Valin and E. Bose, **"**User Information Fusion Decision Making Analysis with the C-OODA Model" *14th on Information Fusion*, Chicago, IL, 2011
**G. Conti, M. Ahamad and R. Norback; "Filtering, Fusion and Dynamic Information Presentation: Towards a General Information Firewall;" *IEEE International Conference on Intelligence and Security Informatics (IEEE-ISI)*; May 2005. **Talk PPT Slides(2.0M))

xix


Contested Collaboration in Human Data Collection for Physics & Human Derived Information Fusion
"Challenges"
Targets Space
T1
T2
Tn
Sensor-1
Sensor-2
Sensor-N
- Align Data
- Associate Data
- Compute Kinematic & ID State Estimates
- Fuse
- Reports level data for commensuration
Targets state & ID
Associate & Combine
Combined Targets state & ID
Human-1
Human-2
Human-H
Issues:
- Reliablilty
-Confidence
- Uncertainty
- Observed which and what
Associate or Individual H Info
-Info Format: Voice or Text
-Translate
- Context/Semantics
- Interpret
- Info Processing and Transmission
Targets state & ID
*Contested Collaboration Can Sabotage Collab.Efforts
Contested observations among observers cause misunderstandings, conflict, and uncertainty by disputing reports
Collaboration (human info fusion) is essential
*D.H. Sonnenwald and L. G. Pierce, "Information behavior in dynamic group work contexts: Interwoven situational awareness, dense social networks and contested collaboration in command and control", Information Processing and Management 36 (2000) pp.461-479


Mobile Agents-based Data Fusion in Jammed (DOS Attack) Distributed Sensor Networks – Issues & Challenges
Processing Element (Manager & Gateway)
Mobile Agent (MA)
Surveillance Region
Sensor nodes
Jammed Area
Jamming Avoidance Itinerary Design *(JAID) algorithm method in Wireless Sensor Networks (WSN)
1. Calculate near-optimal routes for MAs that incrementally fuse the data as they visit the nodes.
2. In the face of jamming on WSN: map jammed sensor areas, and modify the itineraries of the MAs to avoid the jammed area(s) while not effecting the efficient data dissemination from working sensors.
3. Process using a Mobile Agent Routing Algorithm is subject to: Relative distance between sensors Si and Sj, transmitter power of sensors, amount of data collected at each Si, the number of MAs assigned and the number of iterations used to collect data segments for fusion.
*A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, "JAID: An Algorithm for Data Fusion and Jamming Avoidance on Distributed Sensor Networks", Pervasive and Mobile Computing, 2009.

Client-Server vs. Peer-to-Peer (P2P) Networks



P2P Networks Apps: Network Centric Warfare - C2/BM/ISR in Contested Environments (CE)

- Advantage of P2P networks vs. client server/processing element control
  - **Decentralized**: dynamic connectivity among network nodes (peers) treated equally
  - Each node has communications and processing capability
  - **Adaptive** connectivity and discovery, self organizing, ad hoc and scalable
  - **Homogeneous** – connectivity dynamic and transparent to user (virtual network)
  - **Resource Allocation** –efficient P2P "edge-to-edge" node utilization, query results can be propagated to consumers – thus sharing aggregated information
  - **High degree of fault tolerance and to denial-of-information attacks-jamming**

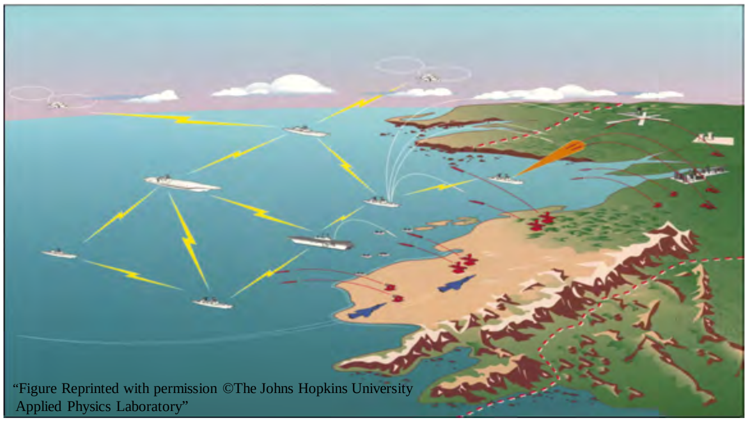
Z.Anwar, W.Yurcik and R. H. Campbell, "A Survey and Comparison of Peer-to-Peer Group Communications Systems Suitable for Network-Centric Warfare", *Defense Transformation and Network-Centric Systems*, edited by Raja Suresh, Proceedings of SPIE Vol. 5820, 2005

A Network Centric Warfare C2/BM/ISR System in CE

- A successful operational system example for C2/BM/ISR, addressing both hostile & environment induced effects of Contested Environments, for air & missile defense applications is the ***Cooperative Engagement Capability (CEC).**
- The CEC system was conceived by Johns Hopkins Applied Physics Laboratory (APL) in the early 1980s and commenced development in 1987 "27 years ago" for the US Navy, with full scale development ready in 1990.
- CEC network in NCW operations is a peer-to-peer (P2P) architecture integrating ships, aircraft and ground based sensor systems.
- P2P connectivity is achieved via dedicated secure wide bandwidth spread spectrum encoded communication systems via adaptive self organizing interconnect phased array antennas on each platform. Data is aligned in time via Cesium clocks at each platform and in space using coordinate transforms/registration, called "gridlock."
- CEC integrates (fuses) and shares aligned local and remote radar sensor measurements and available IFF data to and from all network platforms to form composite target tracks and arrive at a COP at all platforms utilizing platform resident CEC data processors – providing commanders in the network an integrated view of the situation for tasking from selected platforms successfully.
- Overall the system should provide target tracking capability even in areas of denial (jamming, propagation anomalies, weather effects, under attack, etc) and be able to execute defensive weapon launch control targeting functions.

*"The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest*, Vol.16, No.4 (1995), p377-396.

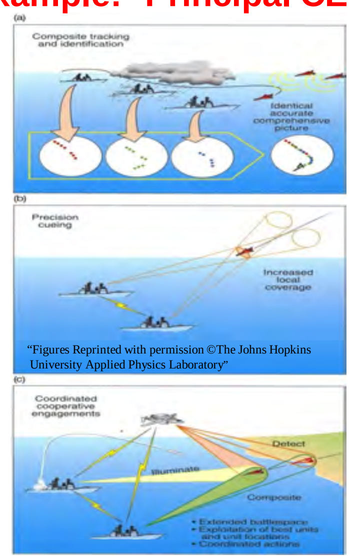
A P2P System for Contested Environment: *Cooperative Engagement Capability (CEC)



"Figure Reprinted with permission ©The Johns Hopkins University Applied Physics Laboratory"

***The littoral battle environment.** Some of the complexities of the environment include friendly, hostile, and neutral forces; advanced cruise missile, electronic warfare, and tactical ballistic missile threats; and a multitude of Allied combatants with multiple sensors and weapons that must be closely coordinated. (Comment: In addition - Areas of denial, jamming, countermeasures, weather, ducting & multipath). **Reference**: *"The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest*, Vol.16, No.4 (1995), p379. "Figures Reprinted with permission ©The Johns Hopkins University Applied Physics Laboratory"

Example: *Principal CEC Functions for COP



"Figures Reprinted with permission ©The Johns Hopkins University Applied Physics Laboratory"

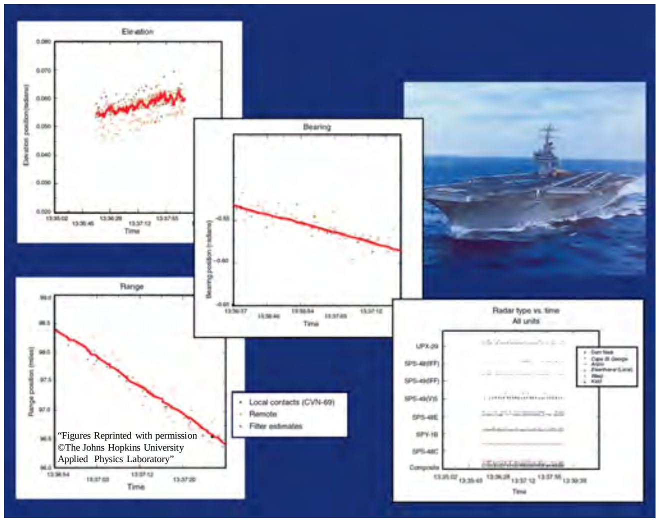
(a) **Composite Tracking**:
Distributing radar measurements data for processing at each unit for composite tracks based on: unfiltered range, bearing, elevation and Doppler updates if available & IFF.

(b) **Precision Cueing**
Facilitates max sensor coverage on any CEC track (using local and remote) with at least one radar with fire control accuracy contributing to the composite track of target. Retention of accuracy is by precision sensor-alignment "gridlock" via local & remote measurements.

(c) **Coordinated, Cooperative Engagements**
Given gridlock, very low time delay & very high update rate, a combatant could fire a missile & guide it to intercept any target using radar data from another CEC unit even if it does not acquire the target with its own radars. This is known as engagement on remote data.

*The principal CEC functions include composite tracking and identification, precision cueing, and coordinated cooperative engagements. (Op.Cit. - above).
Reference:* "The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest*, Vol.16, No.4 (1995), p379.
"Figures Reprinted with permission ©The Johns Hopkins University Applied Physics Laboratory"

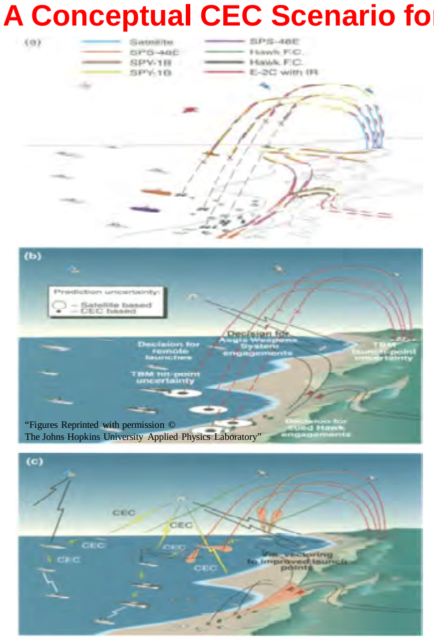
CEC Composite Track Formation Example



*Composite Tracking: Shown are local and remote radar and IFF measurements input to a composite track developed by the CEC onboard the USS Dwight D. Eisenhower

Reference: *"The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest*, Vol.16, No.4 (1995), p388. "Figure Reprinted with permission ©The Johns Hopkins University Applied Physics Laboratory"

A Conceptual CEC Scenario for Ballistic Missile Defense



*This theater scenario illustrates:

(a) detection, cueing, composite track/ID;

(b) coordinated control of engagements and intercepts against threats and their launch points using CEC composite data in conjunction with command/control links; and

(c) engagements/intercepts using composite data.

Reference: *"The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest*, Vol.16, No.4 (1995), p393.
"Figures Reprinted with permission © The Johns Hopkins University Applied Physics Laboratory"

Summary

- There are many issues and challenges remaining requiring research, implementation, testing to validate some of the stated methods. Questions?
- **Addressed:**
  Challenges: The Problem Setting – Cause and effect of Contested Environments; Importance of a systems level approach coupled with fusion applications for defenses; and in Cyberspace aiding of analyst's end-user cognitive functions
- Domains of Contested Environments: Examples of Specific "Effects" and "Defenses", and Associated Methods of Information Fusion
- A Cyber Information Processing System for DOI Defense and Data Analysis
- Cyber DOI Defense: Analyst Cognition Modeling in OODA Loop, and its Relationship to user Data Fusion Information Group (DFIG) Model
- Challenges of Contested Collaboration in Hard and Soft Information Fusion
- Mobile Agents-Based Incremental Data Fusion in Jammed UGS/WSNs
- Importance of Peer-to-Peer (P2) Networks vs. Client Server in C2/BM/ISR
- Example of a successful operational NCW C2/BM/ISR P2P Networked Anti-Jam System in CE: "Cooperative Engagement Capability"

Perspectives on and Applications of Information Fusion in Contested Environments

Ivan Kadar
Interlink Systems Sciences, Inc.
1979 Marcus Avenue, Lake Success, NY 11042

1. INTRODUCTION

This succinct position paper, coupled with the associated viewgraphs, is to highlight: (1) the constituent elements and the "cause and effects" of Contested Environments (CEs), which, to various degrees, have always been considered in systems designs and operations, and (2) the "defensive" role of information fusion. This statement ushers in several "Domains" of CEs, subsets of which are used to illustrate Issues and Challenges, viz. methods of "Defense" ("Winning Strategies") to eliminate/reduce the effects of CEs on operational performance of systems incorporating domain specific applications of information fusion.

The importance of addressing this area has been recently highlighted by the initiation of e.g., two new DARPA programs including: Distributed Battle Management (DBM) and Communications in Contested Environments (CCE) [1]. The DBM initiative is to develop methods to manage complex systems and decision-aiding (HLIF) for air BM, and the CCE program appears to investigate the use of reference architectures for scalable new anti-jam and LPI-like airborne communications networks. The new DARPA programs indirectly address issues depicted in the introduction to panel discussion (see conference program), paraphrasing: "fusion has to address challenges not present in uncontested environments: communications unreliable due to jamming and limited bandwidth providing lower quality/quantity data; sensing may be at stand-off distances and observations sparse; thus fusion may have to deal with potentially distant and stealthy targets, which are difficult to detect". The approaches taken to DARPA programs exemplify need for a "systems level defensive" approach in CE to support the performance of fusion applications.

In this position paper, "Defensive" approaches in CEs are illustrated that use a combination of applications specific CE cognizant systems designs coupled with associated specific fusion algorithms applications towards achieving a specified system performance criterion. That is, fusion applications by themselves cannot be expected to contribute towards the performance goals of the system in CE, unless CE independent situation related information is available.

2. PROBLEM SETTING AND CHALLENGES

Issues and Challenges: Contested environment**s** have always existed with potential deleterious effects on the operation of systems ranging from: space, air, ground and sea operational domains, effecting Command and Control (C2), Battle Management (BM), Intelligence, Surveillance and Reconnaissance (ISR), C2-Comm-ISR (C4ISR), Cyberspace and overall Common Operational Picture (COP), Cyber COP [2] and as well as contested collaboration in C2 (human group contention) [3] effecting soft and hard information fusion. Currently more attention is being paid to CEs to further combat such environments as illustrated in ensuing paragraphs.

Causes and Effects of CEs include: Electronic Warfare (EW): jamming, deception, spoofing, countermeasures; Areas-of-Denial: EW or Environment Induced, Stealth, Kinematic attacks; Information Warfare: Denial-of-Information (DOI) & Denial-of-Service (DOS); Deceptions for Exploitation/DOI (spam, malware, phishing) in Cyberspace; Cyber Warfare (Computer Network Attacks); Contested Collaboration in Command-and-Control (C2) and Social Networks. These are illustrated in a viewgraph depicting the "Domains of CE": Cyberspace, Information, Network and Cyber Warfare [4], Network Centric Warfare (NCW) [5], C2, ISR and BM. Potential "Defensive Approaches" are depicted below.

Issues and Challenges of "Defensive Approaches" described in detail in subsequent paragraphs and in viewgraphs are: (1) Cyber Information Processing System for DOI Defense and Data Analysis specifically addressing needs of intelligence analysts via filtering and info fusion; (2) Cyber DOI Defense: Analyst Cognition Modeling in OODA Loop, and its Relationship to user Data Fusion Information Group (DFIG) Model, augmenting (1); (3) Challenges of

Contested Collaboration in Human Data Collection for Physics and Human Derived (a.k.a. Hard and Soft) Information Fusion [6]; (4) Mobile Agents-Based Incremental Data Fusion in Jammed UGS/Wireless Sensor Networks (WSN) [7]; (5) Importance of Peer-to-Peer (P2P) Networks vs. Client Server [8] for NCW/C2/BM/ISR for adaptive ad-hoc information connectivity; and (6) Example of a highly successful operational NCW C2/BM/ISR P2P Networked Anti-Jam System, subjected to all aspects of Contested Environments, using Measurement Domain Fusion: "Cooperative Engagement Capability (CEC)" [9]. Corresponding slides illustrate the CEC system capability in Littoral battle environments, system functionality and a conceptual scenario with applications of CEC to Ballistic Missile Defense.

3. DEFENSIVE APPROACHES ADDRESSED

3.1. Cyber Information Processing System for DOI Defense and Data Analysis

In 2005 Conti et.al [10] addressed the needs of intelligence analysts to alleviate DOI attacks. Constructed a web based information firewall using a dynamic user customized shared interface and control to increase analyst's decision making effectiveness based on multisource information of many formats and quality through information filtering, fusion and dynamic data transformation to common formats. For detailed description of the method the reader is referred to [10]. The figure entitled "A Cyber Info Processing System Concept for DOI Defense and Analysis" is adapted from [10] but significantly modified from Conti's processing system by including Big Data Analytics-based [11] front-end in the form of Data Mining [12] discovered models of data and learning for acquiring user knowledge base. The information firewall block is analogous to Conti's using user defined rules and parsing algorithms to rule out malicious DOI attacks, but in the current rendition a learned and transformed common formatted database is used. The intelligence analyst can control information by filtering unneeded information based on learned experiences, utilize learned transformed formats and fuse filtered multiple information sources into a single viewable display to optimize decision making ability.

3.2. Representing "Cyber DOI Defense" in the OODA Loop and OODA in Relation to DFIG User Fusion Model

The human analysts perform the decision making processing steps in DOI defense and data analysis. Conti [10] showed the analyst's decision making process can be modeled in the OODA Loop [13] consisting of Observe, Orient, Decide and Act functions. OODA Loop process has been shown to be related to the information fusion "Data Fusion Information Group (DFIG)" User-Fusion Model by Blasch et.al [13], who demonstrated the relation between the two models. The DFIG model fusion levels include: L0-Data Assessment; L1-Object Assessment; L2- Situation Assessment; L3-Impact Assessment; L4-Process Refinement (a component of Resource Management); L5-User Refinement (a component of Knowledge Management); L6-Mission Management (a component of Platform Management) [13]. Figures in the accompanying slide shows an example of Spam processing by the analyst in the OODA loop and the mapping between DFIG and OODA using a modified version of Blasch's [13] OODA model (Op.cit).

3.3. Contested Collaboration in Human Data Collection for Physics and Human Derived Information Fusion

Sonnenwald [3] studied information gathered from simulated battle exercises and from experienced C2 personnel exploring human information behavior in C2. Three facets of behavior emerged: (1) interwoven situational awareness: individual, intragroup and intergroup shared understanding of situations, (2) need for dense social networks for frequent dynamic info exchange among participants about work context and situation, (3) "contested collaboration" when team members maintain an outward stance of cooperation but work to further their own interests, at times sabotaging the collective effort (Op.Cit.) [3]. In hard and soft information fusion [6] context behavior (3) can arise: e.g., when personnel "P1" reports an observation and insists of the presence of a particular target while other observers dispute the finding, yet personnel P1 claims he is correct because he has many years of experience, thus sabotaging the collective effort. The corresponding viewgraph highlights effects of behavior (3).

3.4. Mobile Agents-based Data Fusion in Jammed (DOS Attack) Distributed Sensor Networks

Mpitziopoulos et.al [7] introduced a Mobile Agent (MA) [14] based approach and an associated fusion algorithm employing incremental data fusion for jamming avoidance in distributed Wireless Sensor Networks. This work represents a good example of DOS networks attacks avoidance, and for the applications of incremental data fusion, which method can be adapted to other applications. The accompanying slide illustrates both the problem and the functionality of the method. For the details of the algorithm the reader is referred to [7]. One potential issue with subject model arises when one considers specific type of sensors, i.e., bearing only, and range and bearing measuring sensors with applications to target localization and tracking. For example in the bearing-only case three simultaneous angle measurements are taken from optimum sensor locations, with respect to a GDOP [15] metric, to determine the min MSE position location of a target. These types of applications are not addressed in the model by Mpitziopoulos et.al [7].

3.5. Importance of Peer-to-Peer (P2P) Networks Applications vs. Client Server in NCW/C2/BM/ISR in Contested Environments (CE)

P2P networks have been used first in the commercial/industrial domain [8] and subsequently in NCW C2/BM/ISR [8] and in many other applications [8] because of their advantages properties over client-server networks. As shown in corresponding slide, with P2P, nodes (clients) in a network can bypass the server and exchange information over the network directly. This provides benefits for information exchange between nodes at the edges or at other interconnect nodes where the information is being collected and used. As a matter of fact nodes can appear or disappear (jamming), but the organization of P2P provides adaptability for ad-hoc network nodes forming and use or for using nodes of interest. Properties of P2P are detailed in associated viewgraph and listed herein: decentralized, adaptive, self-organizing, homogeneous, good resource allocation, all nodes treated equally, possesses identical capabilities, and scalable. Therefore, the use of P2P is ideal for C2/BM/ISR applications as depicted in the following section.

3.6. A Network Centric Warfare C2/BM/ISR System in CE: "The Cooperative Engagement Capability (CEC)"[9]

A successful operational system example for C2/BM/ISR, addressing both hostile and environment induced effects of CEs, for air and missile defense apps is the Cooperative Engagement Capability (CEC). The CEC system was conceived by Johns Hopkins Applied Physics Laboratory (APL) in the early 1980s and commenced development in 1987 "27 years ago" for the US Navy, with full scale development ready in 1990. CEC network in NCW operations is a P2P architecture integrating ships, aircraft and ground based sensor systems. P2P connectivity is achieved via dedicated secure wide bandwidth spread spectrum encoded communication systems via adaptive self organizing interconnect phased array antennas on each platform. Data is aligned in time via Cesium clocks at each platform and in space using coordinate transforms/registration, called "gridlock." CEC integrates (fuses) and shares local and remote aligned radar sensor measurements (AZ, EL and Range and available aircraft IFF data) to and from all network platforms to form composite target tracks and to arrive at a COP at all platforms utilizing platform resident CEC data processors – providing commanders in the network an integrated view of the situation for tasking from selected platforms successfully. Overall the system should provide target tracking capability even in areas of denial (jamming, propagation anomalies, weather effects, under attack, etc) and be able to execute defensive weapon launch control targeting functions. For specific details and apps of CEC refer to the associated viewgraphs and to reference [9].

SUMMARY

Issues, challenges, cause and effect and the domain of CE were described. The importance of a systems level defensive approach in CE coupled with fusion applications selection were identified. In Cyberspace aiding of analyst's end-user cognitive functions were highlighted. Specific domains of defenses addressed include: (1) A Cyber Information Processing System for DOI Defense and Data Analysis; (2) Cyber DOI Defense: Analyst Cognition Modeling in OODA Loop, and its Relationship to user Data Fusion Information Group (DFIG) Model; (3) Challenges of Contested Collaboration in Hard and Soft Information Fusion; (4) Mobile Agents-Based Incremental Data Fusion in Jammed UGS/WSNs; (5) Importance of Peer-to-Peer (P2) Networks vs. Client Server in C2/BM/ISR; (6) Example of a highly successful operational NCW C2/BM/ISR P2P Networked Anti-Jam System in Contested Environments: "Cooperative Engagement Capability" employing measurements domain fusion.

REFERENCES

[1] http://www.darpa.mil/Our_Work/STO/

[2] G. Conti, J. Nelson, and D. Raymond. "Towards a Cyber Common Operating Picture", *International Conference on Cyber Conflict (CyCon), Tallinn Estonia, June 2013*

[3] D.H. Sonnenwald and L. G. Pierce, "Information behavior in dynamic group work contexts: interwoven situational awareness, dense social networks and contested collaboration in command and control", *Information Processing and Management* 36 (2000) pp.461-479

[4] M. Miller, J. Brickey, and G. Conti, "Why Your Intuition About Cyber Warfare is Probably Wrong", *Small Wars Journal*, Nov 2012.

[5] D.S. Alberts, J.J. Garstka, and F.P. Stein, "Network-Centric Warfare: Developing and Leveraging Information Superiority," *C^4ISR Cooperative Research Program*, 1999.

[6] I. Kadar, "Issues in Relating Hard and Soft Information for Fusion", presented at Invited Panel Discussion: Real-World Issues and Challenges in Hard and Soft Fusion, Organizer Ivan Kadar, *Signal Processing, Sensor Fusion and Target Recognition XX*, edited by Ivan Kadar, Proc. SPIE Vol. 8050 Orlando Fl., April 2011.

[7] A.Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, "JAID: An Algorithm for Data Fusion and Jamming Avoidance on Distributed Sensor Networks", *Pervasive and Mobile Computing*, 2009.

[8] Z. Anwar, W.Yurcik and R. H. Campbell, "A Survey and Comparison of Peer-to-Peer Group Communications Systems Suitable for Network-Centric Warfare", *Defense Transformation and Network-Centric Systems*, edited by Raja Suresh, Proceedings of SPIE Vol. 5820, 2005

[9] "The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest*, Vol.16, No.4 (1995), p377-396

[10] G. Conti, M. Ahamad and R. Norback; "Filtering, Fusion and Dynamic Information Presentation: Towards a General Information Firewall;" *IEEE International Conference on Intelligence and Security Informatics (IEEE-ISI)*; May 2005. Talk PPT Slides (2.0M)

[11] http://en.wikipedia.org/wiki/Big_data

[12]http://en.wikipedia.org/wiki/Data_mining

[13] E. Blasch, R. Brenton, P. Valin and E. Bose, **"**User Information Fusion Decision Making Analysis with the C-OODA Model" *14th Conference on Information Fusion*, Chicago, IL, 2011

[14] V. Pham, A. Karmouch, "Mobile Software Agents: An Overview", *IEEE Communications Magazine*, Vol. 36, No. 7, pp. 26-37, 1998.

[15] C. Yang, E. Blasch, I. Kadar, "Geometric Factors in Target Positioning and Tracking", *12th International Conference on Information Fusion*, Seattle, WA, July 6-9, 2009.

Fusion in Contested Environments

Chee-Yee Chong
Independent Consultant

SPIE DSS May 2014

1

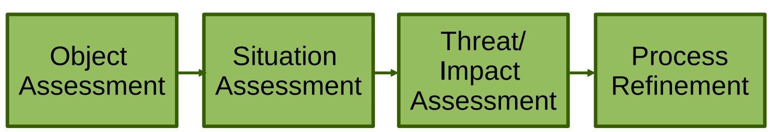
	Problem characteristics	Fusion challenges
Targets	- Highly capable targets with sensing and fusion capabilities - Targets may use countermeasures to avoid detection - Target behaviors may be very different during conflicts	- Low level fusion cannot assume independent targets with simple models - Fusion in gaming situation is immature - High level fusion based on pre-conflict training data may not work during conflict
Sensors	- Standoff sensors may not provide good detection - Sensors may only provide sparse measurements - Sensor models are highly uncertain due to counter-measures	- Fusion has to work with low quality data with poor detection probability - Data association is difficult and requires computing intensive MHT - Learning sensor models in real-time is needed to support fusion
Communication	- Limited communication bandwidth does not allow centralized fusion - Fusion consumers have different information needs	- Distributed fusion is needed to provide consistent operating pictures to users - Communication management is needed to support different users
Human computer interaction	- Large problems with big team of analysts and onboard operators - Fast tempo during conflicts requires real-time response	- Distributed fusion requires mixed automation and human processing - Fusion has to shift between automation and human operators according to tempo

Information Fusion Designed for (Robust) Action

Dr. Jorge E. Tierno
Barnstorm Research Corporation

Barnstorm Research

Classic View of Information Fusion



- A signal processing paradigm
  - Sequential mine and refine
  - Only in the last step is action considered
  - Time is not part of the process
- This approach has been highly successful
  - But current permissive environment key to its success

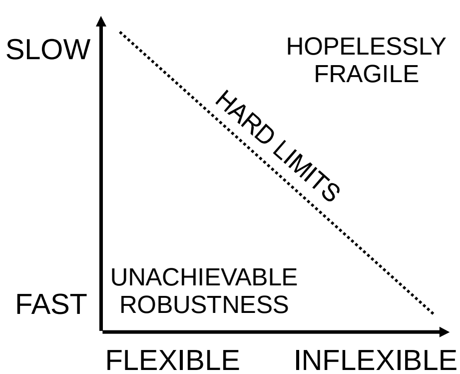
Barnstorm Research 2

The New Challenges

- Distributed sensors/actors
  - Limited/challenged communications
  - Uncertain sensing
  - Limited Access
- Implementing classic fusion in this new environment much harder
- Should we even try?
  - Is achieving the same performance hard or impossible (and counterproductive)?

Barnstorm Research 3

Feedback Systems Have Fundamental Limits

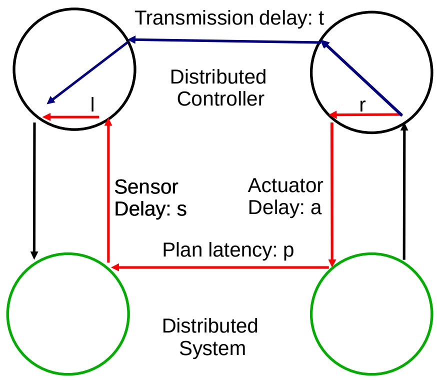


- Robustness cannot be achieved everywhere
  - These are fundamental limits, e.g. Bode's integral
- Designs in top right corner are wasteful in bounded quantities

New Fusion Enterprise Should be Designed to Operate Along Limit Boundary

Barnstorm Research 4

When is Decentralized Control Easy?



If

$$t < r + (a + p + s) + l$$

Then decentralized control design can be made **convex**

A Fusion Enterprise Wired for Action Minimizes Delays

Barnstorm Research

5

A Fusion Enterprise Wired for Action

- Uncertain environments call for robust solutions
  - Robustness is not an add-on
  - Robustness requires tough choices
- Fusion is part of a System-of Systems
  - Fusion enterprise design impacts complexity/capability of SoS
  - Delays are critical

Barnstorm Research

6

Acknowledgements/References

- More on
  - Fundamental Limits for Robustness
    - Doyle, J. C., & Csete, M. (2011). Architecture, constraints, and behavior. Proceedings of the National Academy of Sciences, 108(Supplement 3), 15624-15630
    - http://www.cds.caltech.edu/~doyle/wiki/images/b/b3/UnivLawsArchs.pdf
  - Distributed Control Design
    - Rotkowitz, M., & Lall, S. (2006). A characterization of convex problems in decentralized control. Automatic Control, IEEE Transactions on, 51(2), 274-286

Barnstorm Research

7

Information Fusion Designed for (Robust) Action

Eric Jones[a] and Jorge Tierno[b]

[a]Systems and Technology Research, Woburn, MA, USA;
[b]Barnstorm Research Corporation, Malden, MA, USA

ABSTRACT

Keywords: Multi-int fusion, robust control

1. INTRODUCTION

Information fusion, although always of interest, became a primary focus after the intelligence failures of the early 2000's. The mantra of "connect the dots" gave rise to the development of brand new fusion centers and also to "Total Information Awareness" effort at DARPA. The basis for these efforts was an information theoretic view of the fusion process. The ultimate objective of fusion is to gather all available information, and to process it through a chain of increasingly higher level filters, to achieve as complete as possible a picture of the situation. Implicit in this approach is the assumption that the real operational value of the fusion process is only achieved once that complete picture is formed. It is not coincidence, that the information theoretic fusion approach was developed against a threat operating in our own back yard, or in environments to which we had relatively easy access.

We are now faced with a different environment. One in which our ability to pry is matched or bested by our adversaries ability to conceal. A natural reaction is to attempt to extend the rather successful current view of fusion to this new set of challenges. In what follows, we argue that it may be wise to push against that urge. It may lead us to attempt the impossible, while overlooking good opportunities for progress.

2. A FUSION ENTERPRISE WIRED FOR ACTION

The current approach to fusion has an emphasis on "knowing." The final objective of the fusion process is to understand the intent of our adversaries. Many of the research efforts spawned by the quest to be omniscient relied on elaborate ontologies and patterns of behavior and intent. The price of such an approach is paid in adaptability— the models were cumbersome, hard to produce and extend— and in speed, as accurate conclusions require long observations.

Conflicts of the future will be characterized by distributed agents operating in communication challenged environments, and latency of information will trump completeness. To illustrate this concept, consider another high stakes domain, characterized by near peer adversaries operating in denied environments: investment bank trading. Investment banks have limited visibility into the companies they are trading, and into the behavior of other investors. Exhaustive analysis is one possible approach to this problem. Gather all the available information, build models of companies and stock prices, use those models to build a picture of the market and plan the trades accordingly. On the other hand, the recent book "Flash Boys"[1] explains how, by exploiting communication latencies it became possible for a trading house to achieve the almost impossible, 1200 plus days of money making trades. They did not aim to know everything there was to know about the companies they traded in. They didn't carefully gather and analyze large amounts of data. They simply figured out that they could get ahead of other market agents trades by a millisecond or two and trade in front of them.

Flash traders exchange knowledge completeness for speed. Whatever knowledge they have, they have early enough to act on it, and make a handsome profit in the process. They build an enterprise wired for action. The fusion enterprise in the future should not lose sight of the value of speed over completeness.

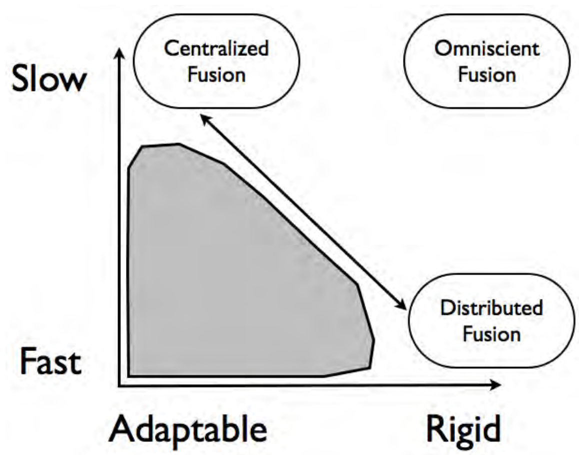


Figure 1. Omniscient Fusion is wasteful in both speed and adaptability. Newer approaches can optimize one or the other.

3. FUNDAMENTAL LIMITS: YOU IGNORE THEM AT YOUR OWN RISK.

There are fundamental limits on how robust a feedback control system can be. The ability of a controller to manage uncertainty and viability is bounded, and designers should be careful not to waste it. Figure 1 shows a cartoon representation of the fundamental limits concerning adaptability and speed of reaction. The grayed out area indicates performance that cannot be achieved.

The purpose of the enterprise architecture, as argued by Doyle[2] is to make it easier to achieve the fundamental limits and to design systems that can be easily made to operate in any point along the boundary of the performance envelope. Robustness of the new fusion enterprise should not be achieved through algorithms alone. The new fusion enterprise should be architected from the ground up, to achieve an optimal robustness tradeoff.

4. RECENT ADVANCES IN CONTROL OF DISTRIBUTED SYSTEMS

High frequency trading is set up for action: The trader's algorithms use the incoming information to determine the next action. Once these actions are taken in milliseconds, without the benefits of human analysis, the algorithms have to be very robust. Small errors would lead to losing large amounts of money. What characteristics make a distributed system easy to control? One way to answer this question is by looking under what conditions the controller design problem is "easy". Recent work by Rotkowitz[3] for example, focuses on finding conditions under which the synthesis problem is convex. One striking conclusion from this body of work is the central role that delay plays in distributed systems.

5. CONCLUSION

The future environment poses multiple challenges to our current fusion enterprise. To meet these challenges we must architect the new fusion enterprise from the ground up to focus on enabling action, robustly, in an environment where latency trumps completeness.

REFERENCES

[1] Lewis, M., [*Flash Boys: A Wall Street revolt*], W. W. Norton & Company, 1 ed. (March 2014).

[2] Doyle, J. C. and Csete, M., "Architecture, constraints, and behavior," *Proceedings of the National Academy of Sciences* **108**(Supplement 3), 15624–15630 (2011).

[3] Rotkowitz, M. and Lall, S., "Decentralized control subject to communication and propagation delays," in [*Decision and Control, 2004. CDC. 43rd IEEE Conference on*], **5**, 4990–4997, IEEE (2004).

Further author information: (Send correspondence to E. Jones)
EJ E-mail:eric.jones@stresearch.com, JT E-mail:jorge.tierno@barnstormresearch.com

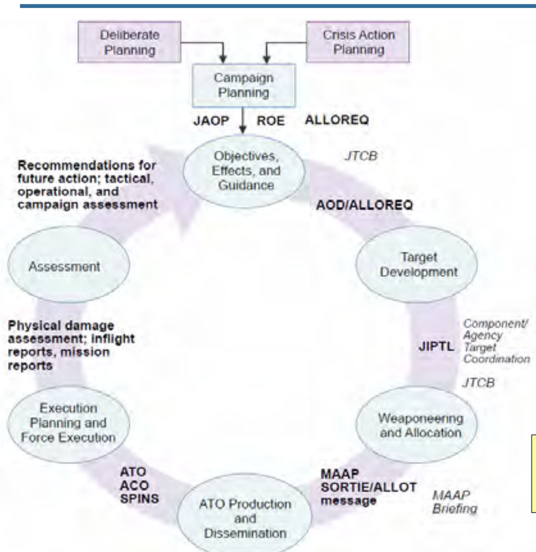
Intelligence, Surveillance, and Reconnaissance (ISR) in Contested Environments

May 5, 2014

Eric K. Jones

1

Air Tasking Cycle



Legend

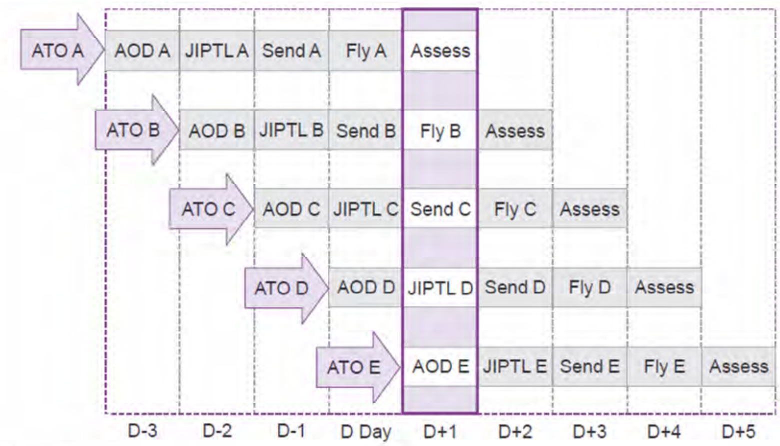
ACO	airspace control order
ALLOREQ	allocation request
ALLOT	allotment
AOD	air operations directive
ATO	air tasking order
JAOP	joint air operation plan
JIPTL	joint integrated prioritized target list
JTCB	joint targeting coordination board
MAAP	master air attack plan
ROE	rules of engagement
SPINS	special instructions

Italic Text	meetings or sub-processes
Bold Text	common products of this phase

AOC acts as a central nexus for ISR collection, integration, and dissemination

Ref: Joint Publication 3-30, p III-21 2

Air Tasking Cycle



Legend

AOD air operations directive
ATO air tasking order
JIPTL joint integrated prioritized target list

Ref: Joint Publication 3-30, p III-20

3

Older Challenges & Adaptations

- Challenges:
  – Fast tempo of adversary dynamics implies that many targets and collections cannot be preplanned
  – Deployment of air assets introduces significant unavoidable latencies (load-out times, flight times)
- Adaptations: Compress rest of the timeline
  – Put loaded plans on ramps, ready for flight
  – Put planes on orbits, ready for “pop-ups”
  – Develop targets and collections while en route
  – Dynamic targeting cell manages these processes

4

Recent Challenges & Adaptations

- Challenges:
  - Complex coordination of multiple assets in real time is often required
  - Information asymmetries sometimes militate against centralized decision-making and control
- Adaptations: Start to modify the enterprise
  - Delegate authority to ground commanders using mission type orders
  - New approaches to use of remotely piloted aircraft
  - Experimentation with “non-traditional ISR”

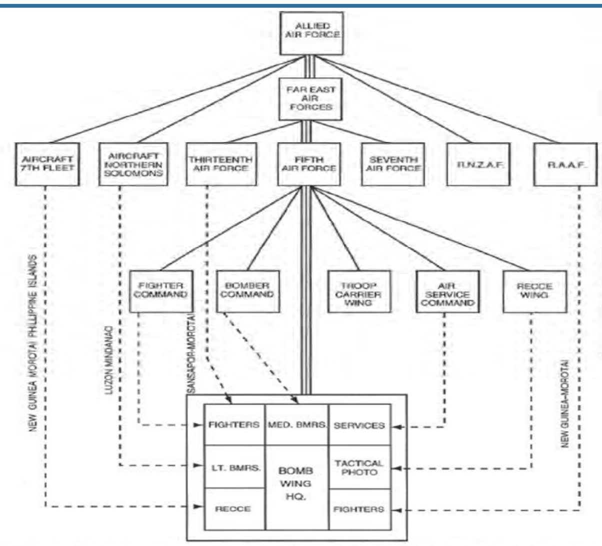
5

Future Challenges & Adaptations

- Challenges of contested environments:
  - Uncertainty regarding threat to forces as well as targets and collections
  - Centralized control may become impossible due to communications disruptions
  - There may be no ground commanders to delegate to
- Possible adaptations: Enterprise transformation
  - Shift operational level battle management forward to wings and even airborne nodes
  - Integration of strike and ISR becomes the norm
  - Small, attritable autonomous unmanned air vehicles provide eyes and ears forward

6

Delegation to Wings is not a New Idea



Source: *United States Strategic Bombing Survey, Pacific War*, vol. 71, *The Fifth Air Force in the War against Japan* (Washington, D.C.: War Department Military Analysis Division, 1947), 10.

7

Conclusions

- We must be prepared for air operations in a contested environment against a peer adversary ...
  - for the first time since World War II
- Centralized control with the AOC as sole information nexus is no longer sufficient
- This will force a more decentralized approach to battle management ...
  - including a much tighter integration of ISR and strike

8

DARPA

System of Systems Distributed ISR

John D. Gorman

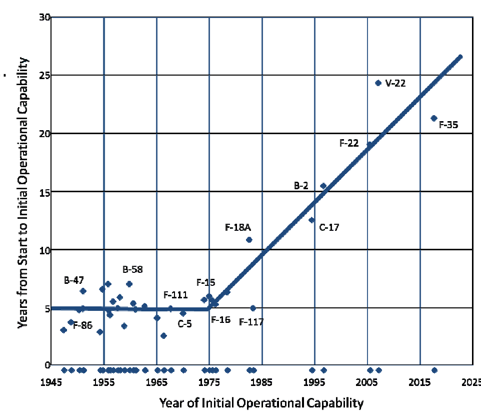
DARPA/STO

May 2014

DARPA

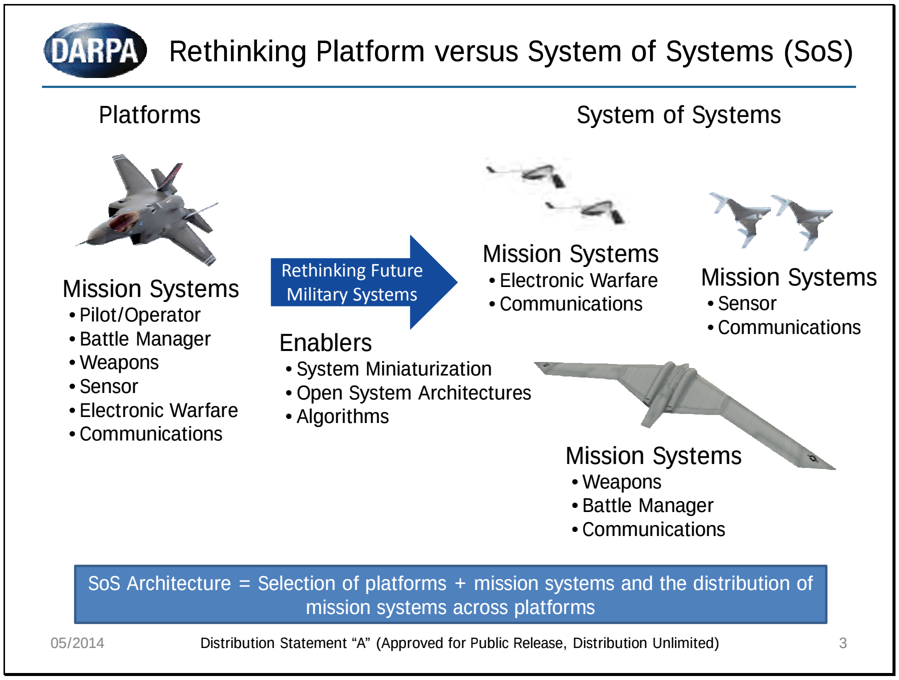
System of Systems Challenge

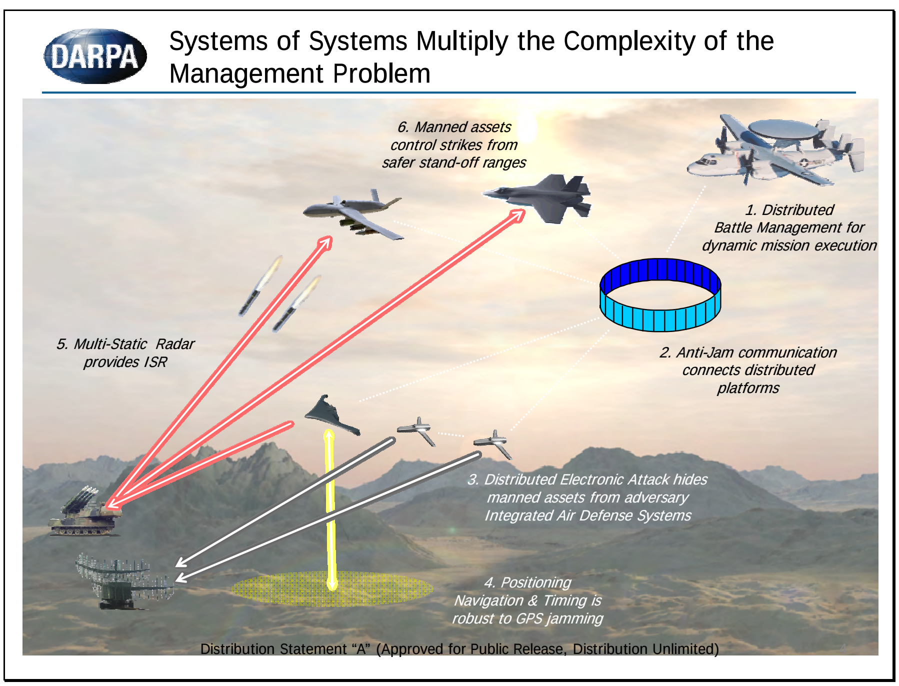
- Peers challenging U.S. dominance of space, air, sea, ground and EM spectrum
  - Investing in technologies to produce high-end systems in large quantities
- US platforms take decades to field...
  - Commercial components obsolete before fielding
- ...and become expensive to buy
  - F-22 buys went from 750 -> 188



The U.S. must re-think how it builds complex military systems

05/2014 2


DARPA
Rethinking Platform versus System of Systems (SoS)
Platforms
System of Systems
Mission Systems
• Pilot/Operator
• Battle Manager
• Weapons
• Sensor
• Electronic Warfare
• Communications
Rethinking Future Military Systems
Enablers
• System Miniaturization
• Open System Architectures
• Algorithms
Mission Systems
• Electronic Warfare
• Communications
Mission Systems
• Sensor
• Communications
Mission Systems
• Weapons
• Battle Manager
• Communications
SoS Architecture = Selection of platforms + mission systems and the distribution of mission systems across platforms
05/2014
Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)
3


DARPA
Systems of Systems Multiply the Complexity of the Management Problem
6. Manned assets control strikes from safer stand-off ranges
1. Distributed Battle Management for dynamic mission execution
5. Multi-Static Radar provides ISR
2. Anti-Jam communication connects distributed platforms
3. Distributed Electronic Attack hides manned assets from adversary Integrated Air Defense Systems
4. Positioning Navigation & Timing is robust to GPS jamming
Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

Developing Systems of Systems

- **Problem** – Near peer threat drives a system of systems approach to incorporate advanced technologies into future systems
- **Hypothesis** – System of Systems approach can increase mission effectiveness, cost leverage, and adaptability by:
  - Distributing functionality across platforms offering favorable capability vs cost trades
  - Embracing wide-spread heterogeneity to reduce vulnerabilities, increase agility, and enable competition for capabilities
- **Approach**
  - Architecture Development and Analysis: develop SoS concepts for prototyping and experimentation
  - Integration Technology Development: develop tools to simplify the integration of new technologies into system of systems architectures
  - Experimentation: demonstrate rapid system integration and military utility to validate SoS performance

05/2014 Distribution Statement "A" (Approved for Public Release, Distribution Unlimited) 5

Panel Discussion – Contested Environments

Erik Blasch,
Mark Pronobis
Mike Hinman
Jim Nagy
Steve Scott

Information Directorate
Activity and Analysis Branch (RIEA)

Contested Environments

Contested
Oppose (an action, decision, or theory) as mistaken or wrong
: to make (something) the subject of a legal case
: to say that you do not agree with or accept (something)
: to try to win (something)
: to struggle or fight for or against someone or something
[Webster]

Environment:
: the conditions that surround someone or something
: the conditions and influences someone or something
[webster]

Conditions of Opposition

2

Contested Environments
Options

Conditions (Previous Panels)

Time = Operate faster (Situation Assessment)
Space = Leverage historical data (HCSB modeling)
Frequency = Use All source information (Sensor Management)
Motivation = Game Theory (Knowledge Representation)

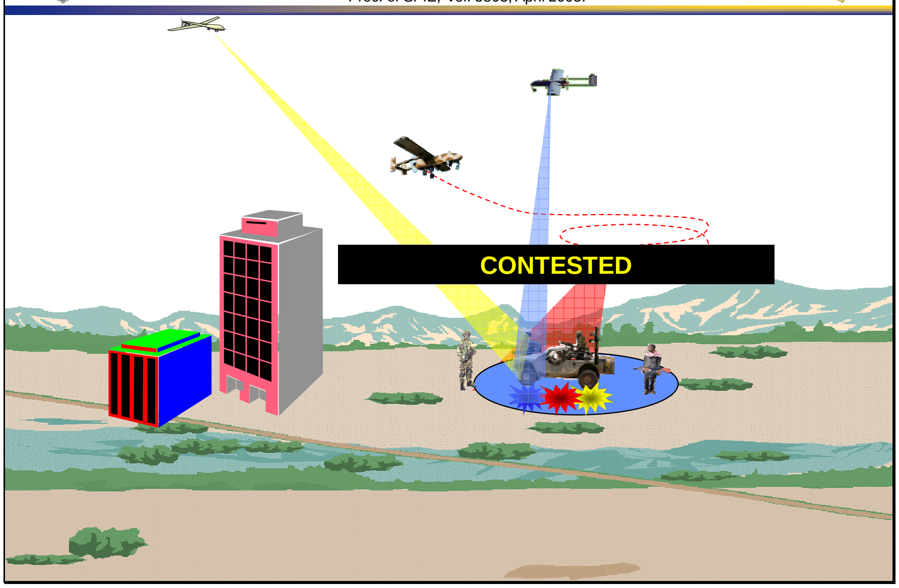
	Time	Space	Frequency	Motivation
All-Source	√	√	√	√
Game Theory	√		√	√
Action	√	√	√	
Knowledge				√
Situation	√	√		√

Conditions of Opposition

3

Scenario

E. Blasch and J. Leonard, "Proactive Sensor Fusion for Urban (SASO) Operations," *Proc. of SPIE,* Vol. 5803, April 2005.



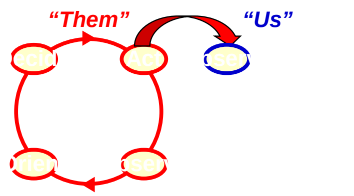
(1) Time: Operate Faster

E. Blasch and J. Leonard, "Proactive Sensor Fusion for Urban (SASO) Operations," *Proc. of SPIE,* Vol. 5803, April 2005.

Fusion - Impact Assessment (JDL Level 3)

ODDA Analysis

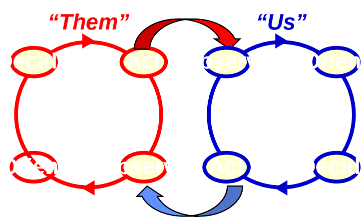
Estimation & prediction of effects on situations of planned or estimated/predicted actions by the participants



Including interactions between action plans of multiple players:

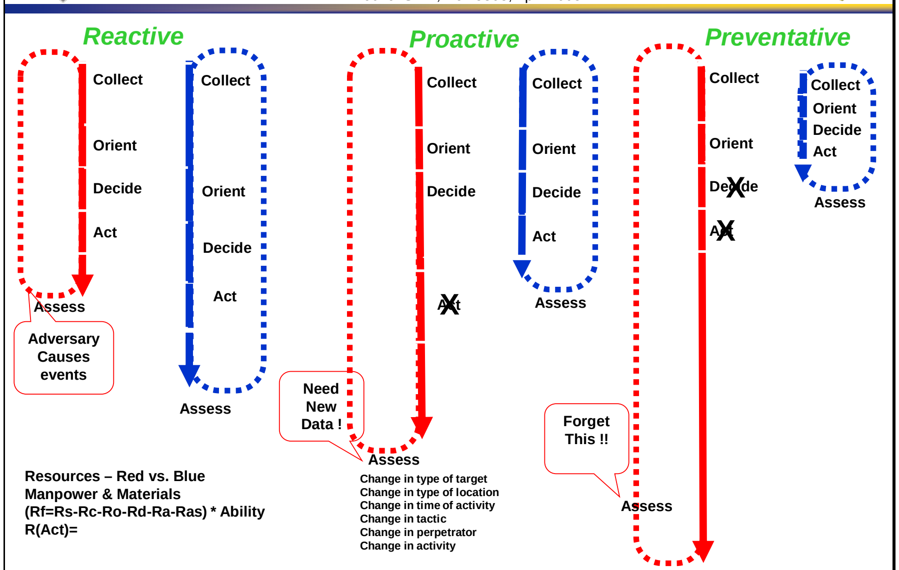
> Assessing susceptibilities & vulnerabilities to estimated/ predicted threat actions given one's own planned actions

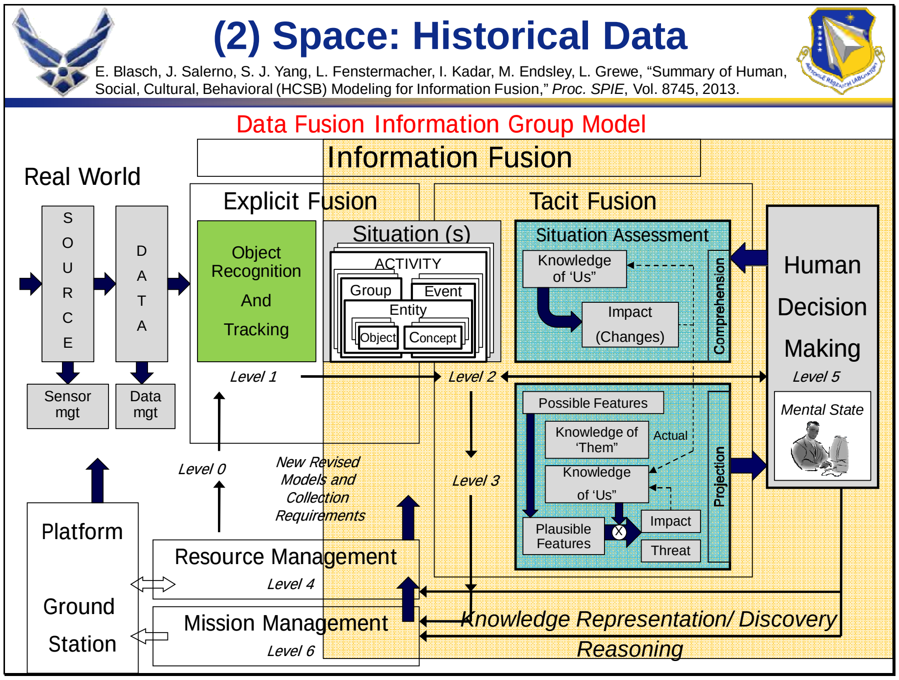
> Effect on own forces and assets of Intended course of action

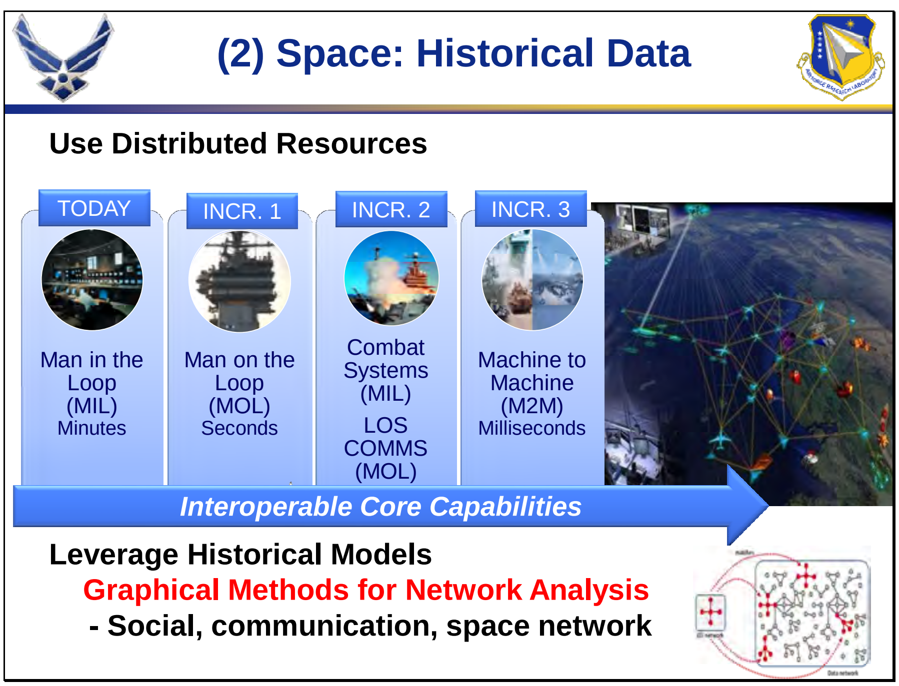


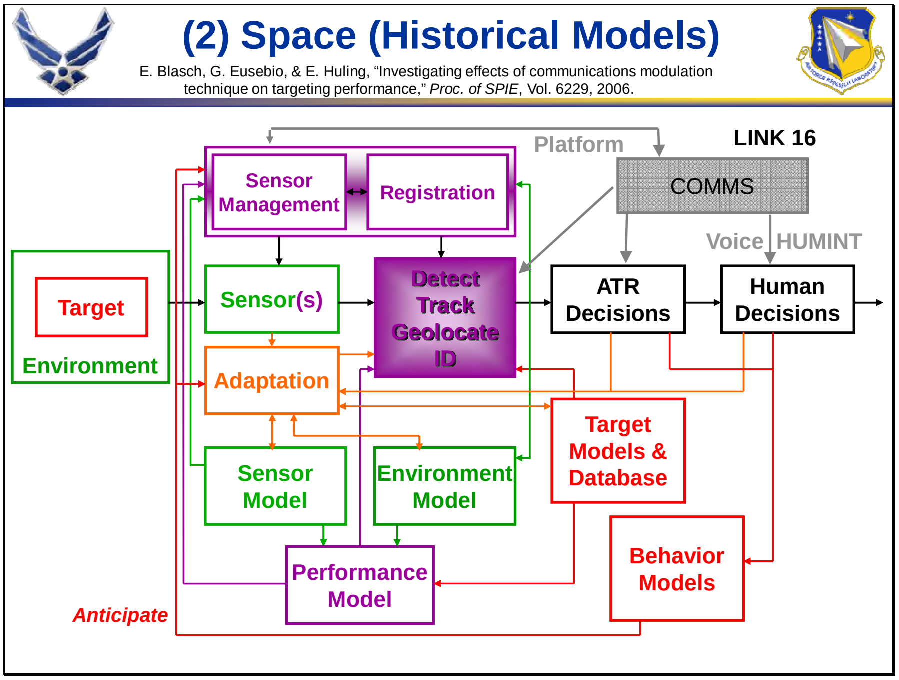
(1) Time: Operate Faster

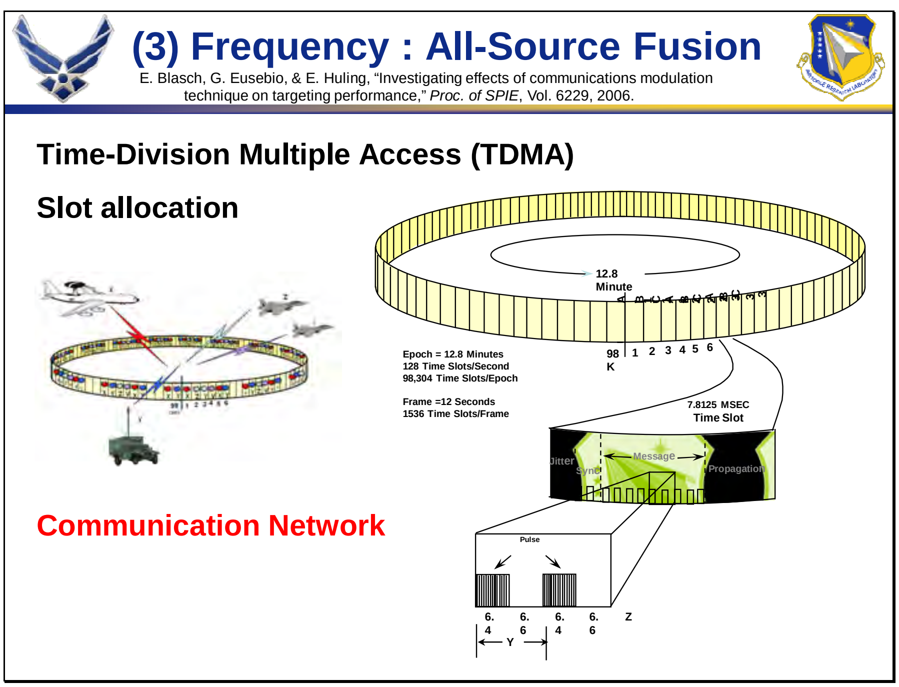
E. Blasch and J. Leonard, "Proactive Sensor Fusion for Urban (SASO) Operations," *Proc. of SPIE,* Vol. 5803, April 2005.




(2) Space: Historical Data
E. Blasch, J. Salerno, S. J. Yang, L. Fenstermacher, I. Kadar, M. Endsley, L. Grewe, "Summary of Human, Social, Cultural, Behavioral (HCSB) Modeling for Information Fusion," Proc. SPIE, Vol. 8745, 2013.
Data Fusion Information Group Model
Information Fusion
Real World
SOURCE
DATA
Explicit Fusion
Tacit Fusion
Object Recognition And Tracking
Situation (s)
ACTIVITY
Group
Event
Entity
Object
Concept
Situation Assessment
Knowledge of 'Us"
Impact (Changes)
Comprehension
Human Decision Making
Level 5
Mental State
Level 1
Level 2
Sensor mgt
Data mgt
Possible Features
Knowledge of 'Them"
Actual
Knowledge of 'Us"
Plausible Features
Impact
Threat
Projection
Level 0
New Revised Models and Collection Requirements
Level 3
Platform
Ground Station
Resource Management
Level 4
Mission Management
Level 6
Knowledge Representation/ Discovery
Reasoning

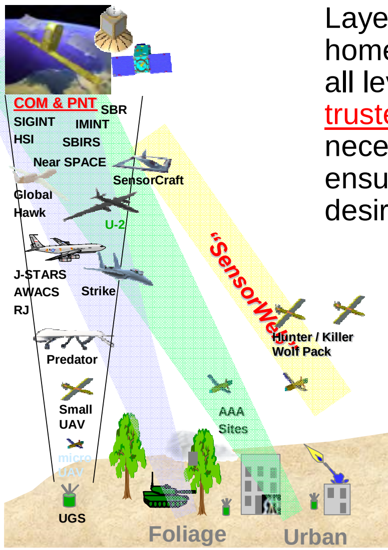

(2) Space: Historical Data
Use Distributed Resources
TODAY
Man in the Loop (MIL) Minutes
INCR. 1
Man on the Loop (MOL) Seconds
INCR. 2
Combat Systems (MIL)
LOS COMMS (MOL)
INCR. 3
Machine to Machine (M2M) Milliseconds
Interoperable Core Capabilities
Leverage Historical Models
Graphical Methods for Network Analysis
- Social, communication, space network


(2) Space (Historical Models)
E. Blasch, G. Eusebio, & E. Huling, "Investigating effects of communications modulation technique on targeting performance," Proc. of SPIE, Vol. 6229, 2006.
Platform
LINK 16
COMMS
Voice
HUMINT
Sensor Management
Registration
Target
Environment
Sensor(s)
Detect Track Geolocate ID
ATR Decisions
Human Decisions
Adaptation
Target Models & Database
Sensor Model
Environment Model
Performance Model
Behavior Models
Anticipate


(3) Frequency : All-Source Fusion
E. Blasch, G. Eusebio, & E. Huling, "Investigating effects of communications modulation technique on targeting performance," Proc. of SPIE, Vol. 6229, 2006.
Time-Division Multiple Access (TDMA)
Slot allocation
12.8 Minute
Epoch = 12.8 Minutes
128 Time Slots/Second
98,304 Time Slots/Epoch
Frame =12 Seconds
1536 Time Slots/Frame
7.8125 MSEC Time Slot
Jitter
Sync
Message
Propagation
Pulse
Communication Network

(3) Frequency : All Source Fusion

From M. Bryant et al , "Layered Sensing Attributes", *2008 (from Web)*
www.wpafb.af.mil/shared/media/document/AFD-080820-005.pdf



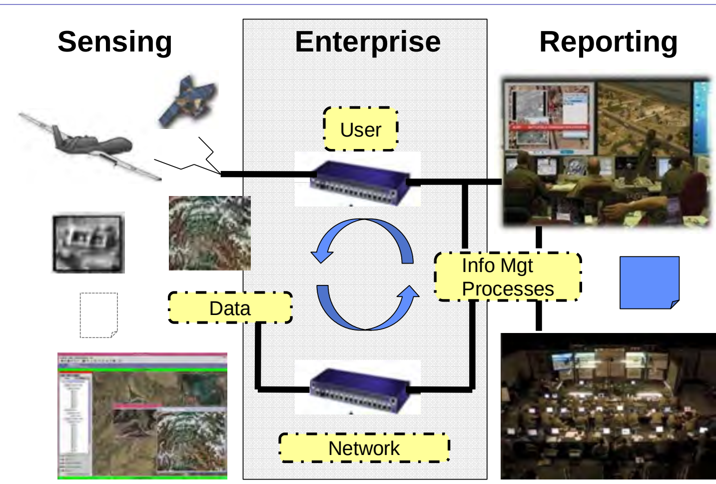
Layered Sensing provides military and homeland security decision makers at all levels with timely, actionable, trusted, and relevant information necessary for situational awareness to ensure their decisions achieve the desired military/humanitarian effects.

Layered Sensing is characterized by the appropriate sensor or combination of sensors/ platforms, infrastructure and exploitation capabilities to generate that situation awareness and directly support delivery of "tailored effects."

(3) Frequency - All-Source Fusion

E. Blasch, O. Kessler, J. Morrison, J. F. Tangney, and F. E. White, "Information Fusion Management and Enterprise Processing." *IEEE National Aerospace and Electronics Conf. (NAECON)*, 2012.

Collection (Processing) ←→ **Analysis** (Exploitation) ← → **Production** (Dissemination)



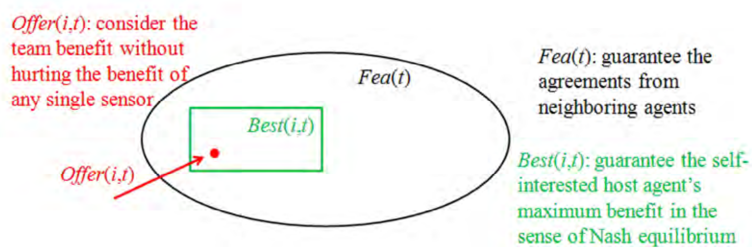
DISTRIBUTION A: E. Blasch, G. Seetharaman, et al, "Wide-Area Motion Imagery (WAMI) Exploitation Tools for Enhanced Situation Awareness ," *IEEE Applied Imagery Pattern Recognition Workshop*, 2012.

(4) Motivation: Game Theory

D. Shen, G. Chen, E. Blasch, K. Pham, P. Douville, C. Yang, and I. Kadar, "Game-Theoretic Sensor Management for Target Tracking," *Proc. of SPIE*, Vol. 7697, 2010.

Game Theory

- **Nash Equilibrium** = no player has anything to gain by changing only his or her own strategy (i.e., by changing unilaterally)
- **Subgame Perfect Equilibrium** is an attempt to choose from the set of Nash equilibria and in every subgame

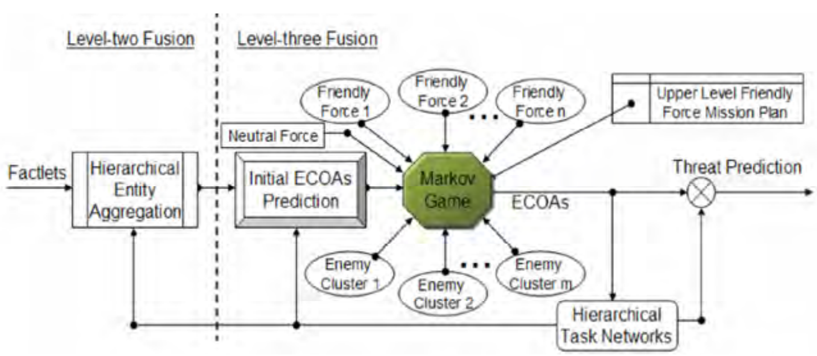


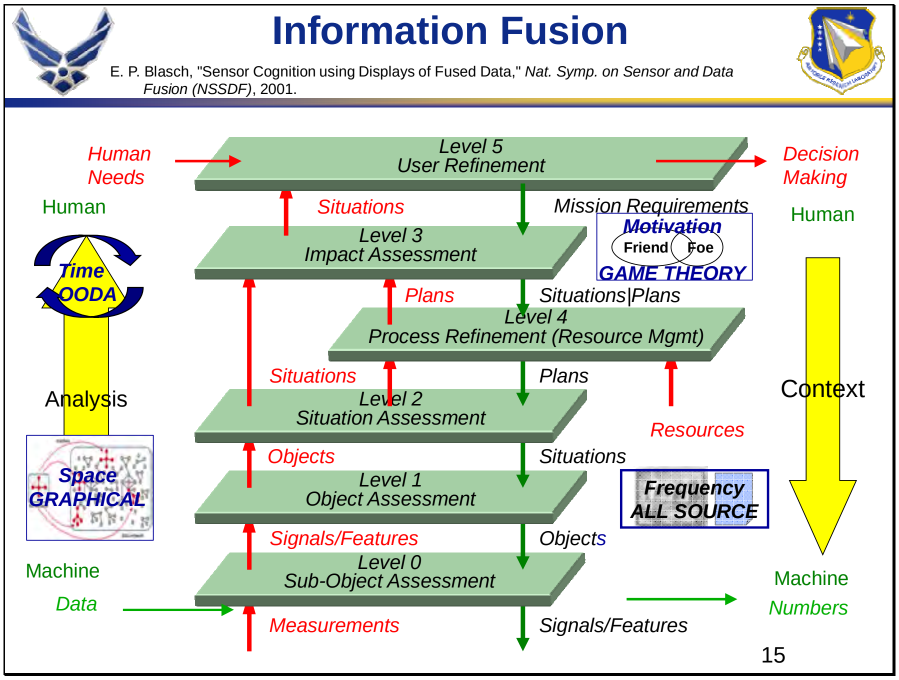
(4) Motivation: Game Theory

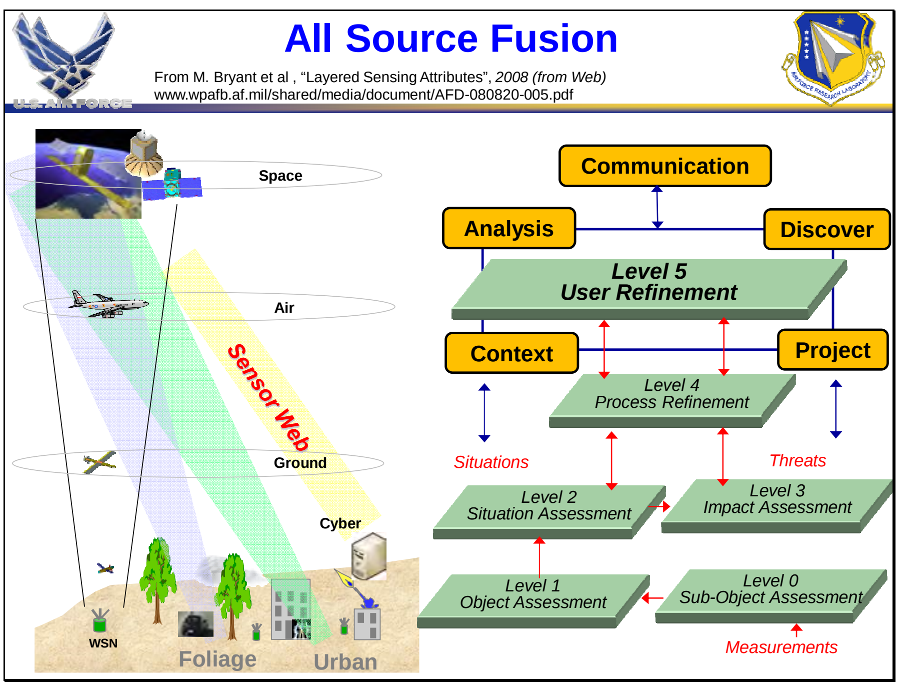
G. Chen, D. Shen, C. Kwan, J. Cruz, M. Kruger, and E. Blasch, "Game Theoretic Approach to Threat Prediction and Situation Awareness," *Journal of Advances in Information Fusion,* Vol. 2, No. 1, 1-14, June 2007.

Game Theory

- **Level 3 Fusion :** Threat Prediction
- **Competing resources:** Cyber, Sensor Management, Tracking

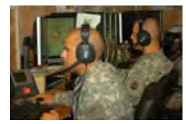



Information Fusion
E. P. Blasch, "Sensor Cognition using Displays of Fused Data," Nat. Symp. on Sensor and Data Fusion (NSSDF), 2001.
Human Needs
Level 5
User Refinement
Decision Making
Human
Situations
Mission Requirements
Motivation
Friend
Foe
GAME THEORY
Human
Level 3
Impact Assessment
Time
OODA
Plans
Situations|Plans
Level 4
Process Refinement (Resource Mgmt)
Situations
Plans
Analysis
Level 2
Situation Assessment
Context
Resources
Objects
Situations
Space
GRAPHICAL
Level 1
Object Assessment
Frequency
ALL SOURCE
Signals/Features
Objects
Machine
Level 0
Sub-Object Assessment
Machine
Data
Numbers
Measurements
Signals/Features
15


All Source Fusion
From M. Bryant et al , "Layered Sensing Attributes", 2008 (from Web)
www.wpafb.af.mil/shared/media/document/AFD-080820-005.pdf
U.S. AIR FORCE
Space
Air
Sensor Web
Ground
Cyber
WSN
Foliage
Urban
Communication
Analysis
Discover
Level 5
User Refinement
Context
Project
Level 4
Process Refinement
Situations
Threats
Level 2
Situation Assessment
Level 3
Impact Assessment
Level 1
Object Assessment
Level 0
Sub-Object Assessment
Measurements

Contested Environments

- **Conditions of Opposition**
  – **Faster**: Multiple OODA loops against time
  – **Historical Data** : Discover to account for space
  – **All-Source Fusion**: Diversity to prepare for limited frequency
  – **Game Theory**: Assess actions conditioned on motivation
- **All-Source Fusion**
  – Other data sources
  – Prepare for disruptions
  – Deal with conditions of opposition



Physics/Human-derived Fusion

Information Fusion for Contested Environments

Erik Blasch[1], Mark Pronobis[1], Mike Hinman[1], Jim Nagy[1], Steve Scott[1]

[1]Air Force Research Laboratory, Information Directorate, Rome, NY, 13441

ABSTRACT

Contested environments pose an interesting challenge for a networked society. We assume that contested means a competition, struggle, or conflict for resources between actors. A competition for resources could be direct such as connectivity rivalry for limited bandwidth, concealment of activities, or jamming access to resources. Contested situations could also be indirect such as loss of connectivity from the environment, obscurations for perception, and communication failures. In each of these examples, it is a loss, or even a degradation of an expected performance from an ideal system from causal/non-causal relations. To solve the contested environment challenge, we can use methods of information fusion of data analytics, contextualization for situation assessment, discovery of relevant information, and projection of information needs towards finding available information when a contested situation exists. A driving paradigm from economics, as a paradigm in social networks, includes game-theoretical solutions.

Keywords: Contested Environments, Information Fusion, Analysis, Discovery

1. CONTESTED ENVIRONMENTS

Contested situations could be based on the competitor actions [1], restriction of access [2], and attacks [3]. Various situational effects could lead to contested environment data limitations. Competitor actions could come via different Observe, Orient, Decide, Act (OODA) loop players which limit data availability. In other cases, access to information could be restricted from environmental effects such as natural disasters and infrastructure problems where the contest is not direct. In the last case, man-made direct attacks could come from denial of service attacks, identity theft, and jamming. In each of these cases, there is a loss of communication. The communications desired could be over information, sensor or social/cultural networks [4] of which situational assessment is challenged [5].

When traditional data sources are degraded then, elements of multimodal fusion could be used to look for other sources of information. An example is all-source fusion [6], shown in Figure 1, in which the user is collecting and interacting with information from various sources of data networks from sensing to social[7, 8]. The diversity of data collection offers an opportunity to access one source of data when another source is contested. What is needed then are methods of user and process refinement of other sources of data complemented with or derived from; analysis, context, discovery, and projection to deal with the information loss due to a contested environment.

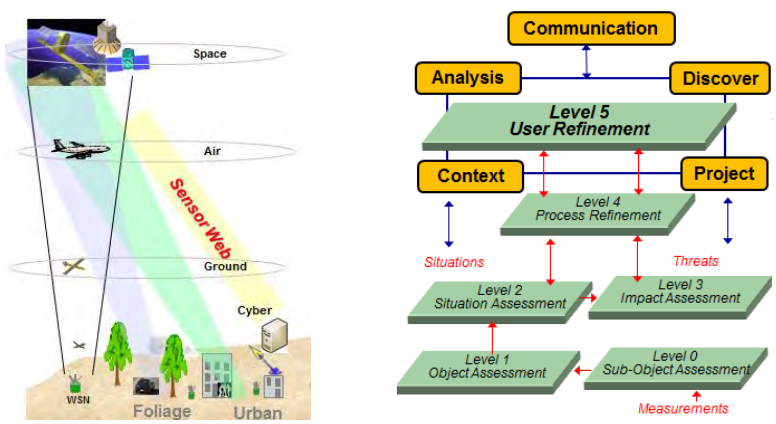


Figure 1: All-Source Sensing and a User refinement-based information Fusion model.

2. ACCEPTED UNDERSTANDING WITH INFORMATION FUSION METHODS

Graphical fusion [9, 10] is a concept of using network analysis to process information to reduce uncertainty. Obviously a contested environment can range from a slight to complete quality or quantity data loss. A user would have to query against multisource data, co-reference different data sources, and determine complementary data through data analytics. Sometimes it would be a user conducting intuitive, inferential, or inductive reasoning versus a user and machine doing passive, routine, or deductive reasoning. A graph (such as a social, communication, or sensor network) could add or utilize context but requires an ontology for uncertainty reduction [11]. A user is required to interpret data and even if physics-based sensing is not available, historical or human-based text reports could be used to further understand the situation.

Accepted understanding of a situation is required when a user deals with the unavailability of information due to time, space, and frequency constraints. In addition to real-time data sensing, knowledge could be gained from historical data. For example, human, cultural and social behavioral (HCSB) modeling could be utilized to determine the situation [12]. If one has a template, patterns, and a priori data; then query by example could be used to assess the available information to augment understanding in the contested environment (e.g., Bayes Net) [13].

Current trends in information fusion include game theory modeling, [1-3], cloud computing [14], data repurposing [15], sparse-data processing [16], machine analytics [17], and multi-intelligence fusion [18]. These developments are applicable to contested environment situations as coordinated with other information sources. Information sources could include open, historical, and human-derived data [19], as well as signals of opportunity [20] to augment physics-based sensing limitations.

Acknowledgements

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of Air Force Research Laboratory, or the U.S. Government.

REFERENCES

[1] Blasch, E., Plano, S., ""Proactive Decision Fusion for Site Security," *Int. Conf. on Info Fusion*, (2005).
[2] Chen, G., Shen, D., Kwan, C., Cruz, J., *et al*., "Game Theoretic Approach to Threat Prediction and Situation Awareness," *Journal of Advances in Information Fusion,* Vol. 2, No. 1, 1-14, June (2007).
[3] Chen, H., Chen, G., Blasch, E., Kruger, M., Sityar, I., "Analysis and Visualization of Large Complex Attack Graphs for Networks Security," *Proc. of SPIE*, Vol. 6570, (2007).
[4] Blasch, E., Valin, P., Bosse, E., Nilsson, M., Van Laere, J., Shahbazian, E., "Implication of Culture: User Roles in Information Fusion for Enhanced Situational Understanding," *Int. Conf. on Info Fusion*, (2009).
[5] Blasch, E., Kadar, I., Salerno, J., Kokar, M. M., Das, S., Powell, G. M., Corkill, D. D., Ruspini, E. H., "Issues and Challenges in Situation Assessment (Level 2 Fusion)," *J. of Advances in Information Fusion,* Vol. 1, No. 2, pp. 122 - 139, Dec. (2006).
[6] Kahler, B., and Blasch, E., "Sensor Management Fusion Using Operating Conditions," *Proc. IEEE Nat. Aerospace Elect. Conf.*, (2008).
[7] Blasch, E., and Plano, S., "Level 5: User Refinement to aid the Fusion Process," *Proc. of SPIE,* Vol. 5099, (2003).
[8] Blasch, E., "Situation, Impact, and User Refinement," *Proc. of SPIE,* Vol. 5096, (2003).
[9] Çetin, M., Chen, L., Fisher, J. W. III, Ihler, A. T., Moses, R. L., Wainwright, M. J., and Willsky, A. S., "Distributed Fusion in Sensor Networks – A Graphical models perspective," *IEEE Signal Processing Magazine*, 42-55, (2006).
[10] Blasch, E., Lechuck, G., Burke, D., *et al*., "User Metrics for Graphical Information Fusion," *Proc. of SPIE*, Vol. 9091, (2014).
[11] Costa, P. C. G., *et al*., "Towards Unbiased Evaluation of Uncertainty Reasoning: The URREF Ontology," *Int. Conf. on Info Fusion*, (2012).
[12] Blasch, E., Salerno, J., Yang, S. J., Fenstermacher, L., Kadar, I., Endsley, M., Grewe, L., "Summary of Human, Social, Cultural, Behavioral (HCSB) Modeling for Information Fusion," *Proc. SPIE*, Vol. 8745, (2013).
[13] Blasch, E., Bosse, E., and Lambert, D. A., [*High-Level Information Fusion Management and Systems Design*], Artech House, MA, (2012).
[14] Blasch, E., Chen, Y., Chen, G., Shen, D., Kohler, R., "Information Fusion in a Cloud-Enabled Environment," in Keesook Han, Baek-Young Choi, Sejun Song (Eds.), [*High Performance Cloud Auditing and Applications*], Springer Publishing, (2013).
[15] Steinberg, A. N., Bowman, C. L., Haith, *et al*., "Adaptive Context Assessment and Context Management," *Int. Conf. on Info Fusion*, (2014).
[16] Tian, Z., *et al*., "Compressed Sensing for MIMO Radar: A Stochastic Perspective," *IEEE Stat. Signal Proc. Workshop,* (2012).
[17] Blasch, E., Steinberg, A. N., Das, S., Llinas, J., Chong, C.-Y., Kessler, O., Waltz, E., White, F., "Revisiting the JDL model for information Exploitation," *Int'l Conf. on Info Fusion*, (2013).
[18] Blasch, E., Nagy, J., Aved. A., *et al*., "Context aided Video-to-Text Information Fusion," *International Conf. on Information Fusion*, (2014).
[19] Panasyuk, A., Blasch, E., Kase, S. E., Bowman, E., "Extraction of Semantic Activities from Twitter Data," *Proc. of the Eight International Conference on Semantic Technologies for Intelligence, Defense, and Security* (STIDS), Fairfax, VA, October, (2013).
[20] Yang, C., Nguyen, T., *et al*., "Field Testing and Evaluation of Mobile Positioning with Fused Mixed Signals of Opportunity," IEEE *Aerospace and Electronics Systems Magazine*, (2014).

AFRL

THE AIR FORCE RESEARCH LABORATORY

LEAD | DISCOVER | DEVELOP | DELIVER

Open Source Information: Implications for Information Fusion in Contested Environments

April 2014

Laurie Fenstermacher

Air Force Research Laboratory, 711 HPW/RHXM

Human Centered ISR Research Division

Briefing Roadmap

- **Challenges for Global ISR**
- **Open Source Information**
- **Benefits of Open Source Information**
- **Analysis of Open Source Information**
- **Issues with Open Source Information**
- **Implications for Information Fusion**

2

Challenges for Global ISR

•Need to adapt the global ISR network to a new security environment

•Fusion, storage and use of the data becoming a larger problem – ideally would like a fused product of cyber, HUMINT, other data

•AF won't always own the platform -- the generated knowledge is (social) context-dependent for a given scenario…TwitterINT overlooked

Challenges for Global ISR

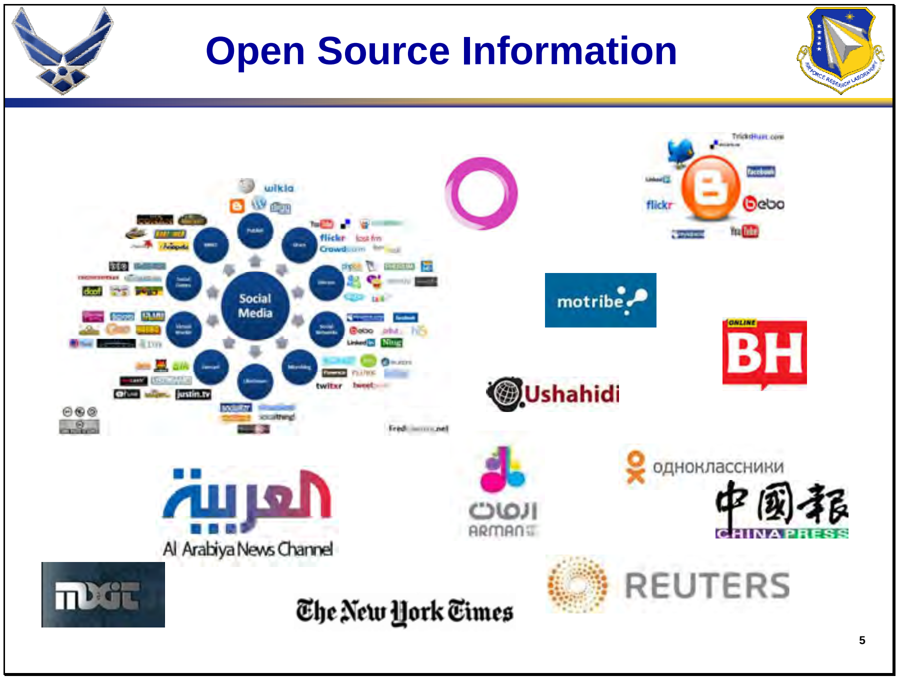
❖Anti access, area denial poses challenges, including limiting the use of "go-to" platforms such as Reaper

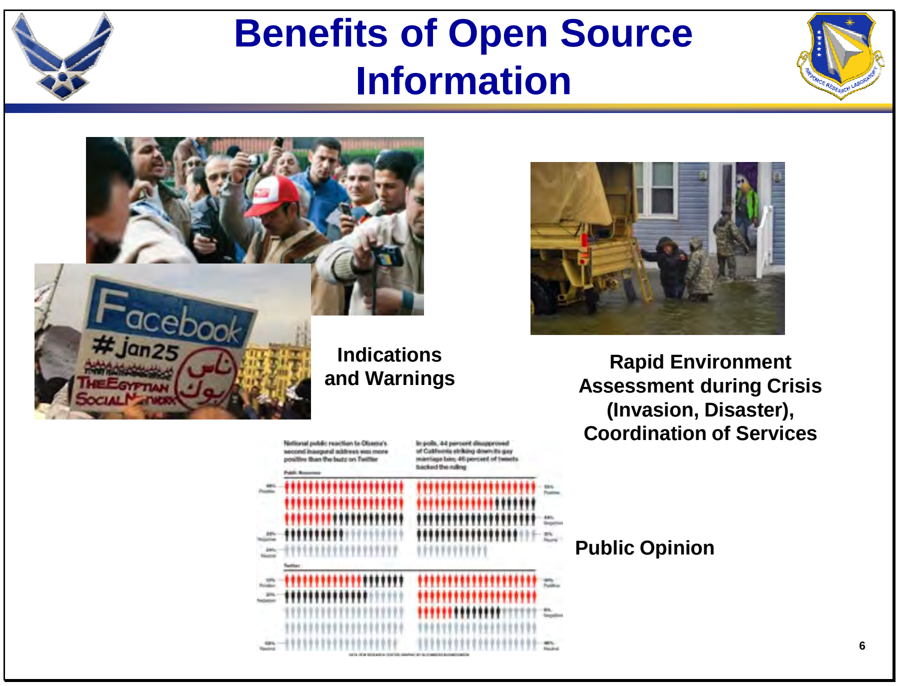
❖ Complexity of security environment drives the need for developing a contextualized and nuanced understanding of the human environment

"*Context is king. Achieving an understanding of what is happening – or will happen – comes from a truly integrated picture of an area, the situation and the various personalities in it. It demands a layered approach over time that builds depth of understanding.*"

LGen Flynn and BGen Flynn, "Integrating Intelligence and Information"

lv


Open Source Information
Social Media
motribe
Ushahidi
BH
одноклассники
中国報
CHINA PRESS
العربية
Al Arabiya News Channel
REUTERS
The New York Times
5


Benefits of Open Source Information
Facebook
#jan25
Indications and Warnings
Rapid Environment Assessment during Crisis (Invasion, Disaster), Coordination of Services
Public Opinion
6

lvi

Benefits of Open Source Information: Area Denial - Monitoring

Some results of brainstorming at recent Social Media Workshop…

- Information collection in countries with high social media presence
  - Iran, China, Venezuela
  - North Korea, Cuba are infeasible…now
- Could effectively crowdsource the CIA fact book
  - Baseline, then measure the deltas
  - Dynamic, living assessment in near-real-time, not available elsewhere
- Could detect new events or elements indicating instability
  - Detect indicators/factors of predictive models
    - Fewer delivery trucks; images of empty plates and hunger (from webcams, uploaded videos)
    - What effect are sanctions having?

7

Benefits of Open Source: Area Denial Monitoring (cont'd)

Counter-Deception:

- Corroboration and validation with traditional ISR
  - Example: staged demonstration in front of camera; overhead image shows rest of area is empty
- Corroboration and validation through social media cross-correlation
  - Example: video narrator had wrong dialect/accent for local area
  - Example: something (entity, weather) is inconsistent between (manipulated) image and other social media images
- Can steer open source content – for example, ask for desired content
  - Can pay for it – set up an online market or use bots to influence/guide

http://www.fourandsix.com/photo-tampering-history/

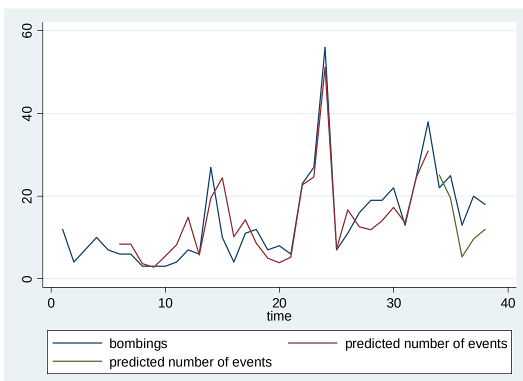
8

Analysis of Open Source Information

- ❑ Volumetric Analysis
- ❑ Sentiment Analysis
- ❑ Language Analysis/Entity extraction
- ❑ Social Network Analysis
- ➢ Meaning Making
  - -- Social Identity
  - -- Integrative Cognitive Complexity
  - -- Worldview Dimensions

Open Source Analysis: Forecasting Violence with Discourse Markers

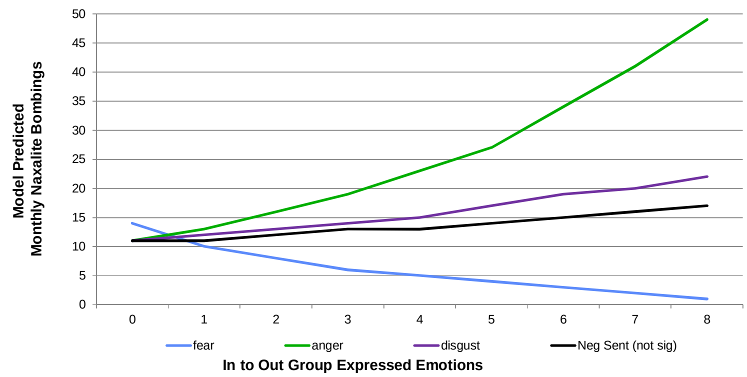
In-Sample Correlation between Fitted Values and Actual Naxalite Bombings = .92
Out-of-Sample Correlation between Fitted Values and Actual Naxalite Bombings = .80



10

lviii

Open Source Analysis: Forecasting based on Changes in Affect



Findings consistent with: Matsumoto's contentions of anger and disgust as telltale signs of violence and social psychological literature re: anger and fear as discrete emotions in terms of effects on behavior

11

Issues with Open Source Information

- **Information validity – misinformation, deception, characterization of automated content generated (e.g., bots)**
- **Source is human; thus, trustworthiness, accuracy, bias (assumptions, value judgements, etc.)**
- **Assessing pedigree, source characterization (Is this representative?)**
- **"Language" variability**
  - **Abbreviations, cryptic texts, emoticons, colloquial, slang, shortcut language (e.g., lol)**
  - **Intentional misspellings**
- **Time and size challenges: dynamic environment – data gets stale, phenomenal growth in amount of data generated**
- **Sparse link structure – sources often not cited**
- **Low "signal-to-noise" (chatter, etc.) -- nearly 45% of Twitter is babble**

12

Implications for Information Fusion

Challenges:

- **Need to systematically and consistently asses the evidence in terms of trustworthiness, pedigree and source characterization**
- **Need to account for and compensate/correct for bias**
- **Need to preserve important contextual information in order to capture nuanced information regarding worldview**
- **Achieving the appropriate synergy between human and computer to truly enable meaning making about threat**

Opportunities:

- **Earlier warning – can improve resource allocation, adjust mental schema**
- **Enables anticipatory information collection, reasoning, forecasting and effective action**

"Predicting…is impossible, but imagining a variety of futures is helpful." **G. Yonas**

Questions?

Laurie.fenstermacher@us.af.mil

937-255-0879

14

Open Source Information: Implications for Information Fusion in Contested Environments

Laurie Fenstermacher
Air Force Research Laboratory, 711 HPW/RHXM, 2255 H Street,
Wright Patterson AFB, OH 45433

ABSTRACT

Gathering information in anti-access, area denial locations will require new ways to collect and interpret information. It will also require a new emphasis on certain sources of information; for example, open source information (including the sources of information labeled "social media"). Open source information (including social media) can provide information on emergent behaviors (e.g., group mobilization), influential persons within a network and can be used to forecast future behaviors and events. Various analytic approaches exist or are being developed to make use of open source information, including social network analysis, language/sentiment/affect processing, statistical (correlational) analysis, behavior modeling and simulation, but gaps remain in enabling humans to do meaning making from the information, including meaning regarding threat. Open source information inherently comes from humans and thus there are a variety of issues: bias, trustworthiness, accuracy, representativeness. All of that makes it difficult to do source characterization and establish pedigree. Further, there is a natural tendency to discount or weight open source information less highly than information from traditional intelligence sources. Open source information provides important context for understanding a situation or threat, interpreting patterns and uncovering hidden meaning and elucidating the worldview of the individual and/or group; thus, any information fusion method should preserve salient contextual information.

Keywords: information fusion, fusion, open source information, social media, meaning making, sensemaking

1. INTRODUCTION

In a recent interview Lieutenant General Larry D James, the Air Force chief of Intelligence, Surveillance and Reconnaissance (ISR), talked about the challenges for ISR post-Afghanistan. He talked of needing to adapt the global ISR network to a new security environment, stating that the focus should be on data (versus platforms) – where it comes from, where to put it and how to use it quickly and decisively. He identified fusion, storage and the use of data as a growing problem and stated that he would like a product that fused cyber, human intelligence and the other data across the network, including data from platforms not owned by the government that often get overlooked, such as "Twitter-INT". LtGen James also discussed new ISR challenges, for example operations in countries sheltered behind formidable anti-access, area-denial systems, commenting that the Reaper could be modified with new sensors, capabilities and greater range, but fundamentally remains an asset that functions better in uncontested environments.[1] The logical question is "what assets/capabilities will fill the gaps left by eliminating, or greatly reducing, the use of close-in platforms like Reaper?" Certainly there are space assets that can be brought to bear and existing sensor systems can be modified to extend their range. The inability or decreased ability to collect certain kinds of data and the inability to process the crucial information available outside traditional intelligence source[2] coupled with the complexity of the current security environment will require a sophisticated, integrated approach. Humans are adaptive, sometimes deceptive, innovative and often unpredictable. Identifying and monitoring emerging threats, interpreting the significance in changes in actors and situations, assessing patterns of life and making meaning about intent requires a tomographic perspective based on a variety of information sources.

2.0 Open Source Information

Open source information is defined as publically available information; that is, information that anyone can lawfully obtain by request or observation. Open source information includes other unclassified information that has limited public distribution or access as well as information used in an unclassified context which does not compromise national security.[4] Open source information is transmitted through newspapers, radio, television as well as email, commercial databases or portable electronic media.

Social media is a subset of open source information. Social media enables/fosters publishing, (e.g., mahalo, livejournal, wordpress, blogger), sharing (e.g., tumblr, YouTube, Pinterest, vimeo), discussing (e.g., reddit, kik, quora, myspace) and networking (e.g., tagged, viadec, mixi, Linkedin) and combinations of these functions (e.g., Facebook, Google+).[5] The types of social media used varies geographically; for example, Odnokassniki is more popular than Facebook in Russia, Orkut is popular in India and Pakistan, Motribe and MXit are popular in Africa and homegrown social media sites (e.g., QQ) are encouraged in China .[6] The content of social media can be characterized as either user generated content or user created content where the key difference between the two is that user created content was created or adapted (i.e., users add value to the work) not merely repeated or copied. Social media is one example of "big data" due to the velocity (frequency of data generation), variety (different data sources) and volume[7]; however, social media are unique in terms of the massive volume generated, the huge variety of multimedia content, the complex, interconnected content structure and the user driven nature of the content.[8]

2.1 Why Use Open Source Information?

Lieutenant General Flynn stated that, "complementary unclassified and open source intelligence can often be better than what we have in the classified domain. The fusion and analysis of open source information with other forms of classified materials is essential to understanding the operational environment…Context is king. Achieving an understanding of what is happening – or will happen – comes from a truly integrated picture of an area, the situation and the various personalities in it. It demands a layered approach over time that builds depth of understanding."[9] Open source information can enable an understanding of geographic and civil factors (e.g., capabilities, logistics, availability of resources) needed for planning and force employment.[10] In situations in which "winning the hearts and minds" is the objective versus solely focusing on demonstrating achieving effects through kinetic operations, it is important to be able to assess perceptions and opinions. Media analysis provides opportunities for understanding, awareness and agility in response, often faster and with less resources.[11] Social media can be used to understand the structure of social networks and their dynamics, identify key people and relationships for insights on influence and cohesion, determine the proliferation of ideas in networks and understand and forecast behaviors and/or events.[12]

More importantly, open source information provides an important window into the human environment, what they're thinking about themselves and others (social identity) and what they're likely to do. Open source information provides perspectives of people: individuals, groups, organizations, societies. Perspectives are not the same as perceptions, but rather are guides to perceptions. Perceptions are based on how humans perceive or define their situations; how they make meaning in the world. Perspectives and perceptions form the lens through which a person or group's reality is filtered -- worldview. Worldview is the socio-culturally, historically, influenced conceptual framework used to make sense or meaning of, describe and interpret reality in terms of what is, an explanation of where it all came from, and what ought to be. This conceptual framework encompasses a set of beliefs that includes limiting statements and assumptions regarding what are good and evil and what objectives should be sought. The beliefs shape what behaviors and relationships are desirable or undesirable in pursuit of objectives. Thus worldview defines the objectives sought as well as the means to achieve them (what ought or ought not to be done).[13] Bottom line? Open source information provides a mechanism to have an "emic" perspective (from the perspective of the "other") – critical for assessing threat and determining intent.

2.2 Analysis of Open Source Information

A variety of techniques exist to analyze open source information, including social network analysis, language/sentiment/affect analysis, statistical (correlational) analysis, volumetric analysis (e.g., social media correlational analysis focused on tweets and events), and behavior modeling (e.g., agent based modeling of group dynamics and/or influence).[14] Previous AFRL research has explored a variety of ways to enable meaning making based on open source (including social media) information. The resulting methodologies and algorithms include algorithms to forecast significant shifts in attitudes[15], methodologies to detect and interpret language related to social identity in order to forecast actions (e.g., violence)[16], algorithms to identify changes in affect (e.g., from anger to contempt to disgust) which correlate to changes in behaviors (e.g., repression, violence)[17,18,19] and algorithms to forecast and understand intent based on social identity and integrative cognitive complexity[20].

2.3 Issues with Open Source Information

There are several issues related to the use of open source information, including social media. First, there are issues with the validity of the data: misinformation, deception and characterization of automated content generated (e.g., by "bots").[21] The source(s) of the information are humans, immediately bringing up issues with trustworthiness and/or accuracy of the information. In addition, because the source is human, the information is based on perspective, inherently a bias containing assumptions, value judgments and ideas[22]. The challenges involved in the analysis, processing and/or characterization of open source information include assessing the pedigree and the representativeness of the information (.e.g, is a Facebook post characteristic of an individual or a group or culture to which they belong or is there bias or deception involved?). In addition, there are processing challenges related to the "language" used (e.g., emoticons, multiple languages, jargon, sarcasm, etc.) In the case of social media, there are also issues of "signal-to-noise"; that is, many social media information sources are very noisy. For example, in certain information sources (e.g., Twitter) there is a great deal of repetition or redundancy in the information resulting, in many cases, the potential for biased assessments and decisions.

3.0 Implications for Information Fusion

There are some obvious implications for the fusion of open source information with other traditional sources of intelligence. One is the need to systematically and consistently assess the evidence in terms of trustworthiness, pedigree and source characterization. In addition, there is the need to account for and/or compensate/correct for bias inherent in information sources. Because open source information provides important clues regarding worldview, in order to incorporate this into a more nuanced understanding of threat requires a fusion method that will preserve important contextual information.

In addition to presenting some challenges for information fusion, open source information presents some opportunities. Threats come from ideas which are expressed in words, typically well before individuals or groups mobilize or act; that is, individuals/groups will tend to renorm and/or justify their attitudes towards behaviors (e.g., violence) before acting out and those "signals" can often be detected in open source information, providing important cues in order to monitor and collect other information. These signals can be detected in the language of social identity as well as the language of dehumanization.[23] In addition, there are many studies which show significant drops in integrative cognitive complexity (based on an analysis of the language of an individual or group and the assessment of the extent to which it reflects the integration of multiple dimensions or perspectives of an issue/problem or not) prior to hostilities, providing additional evidence to add to other information.[24]

In a think piece about intelligence, Gerry Yonas commented that predicting what a group of society would do – especially in the long term – is impossible, but "imagining a variety of futures is helpful."[25] Ultimately, fusion of open source information with traditional intelligence information in order to detect threat and understand intent in contested environments will require a new "mixed initiative" (computer/human) fusion solution that addresses the issues, but takes advantage of the opportunities presented by having a window into the human environment. Doing so will assist humans in meaning making by informing the development of mental schema and helping them to consider possibilities (collection, analysis, synthesis) and understand connections (people, places, events) in order to anticipate/forecast and act effectively.

REFERENCES

[1] Schantz, M.V., "ISR After Afghanistan," Air Force Magazine 96(1), 22-27 (2013).

[2] Flynn, M.T., Pottinger, M. and Bachelor, P.D., "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Voices From The Field, Center for New American Security, January 2010. www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf.

[3] Steele, R.D., "Open Source Intelligence: What Is It? Why Is It Important to the Military?" www.oss.net/dynamaster/file_archive/040320/.../OSS1997-02-33.pdf.

[4] Director of Central Intelligence Directive 2/12: Community Open Source Program, 1 March 1994. www.fas.org/irp/offdocs/dcid212.htm.

[5] Cavazza, F., "Social Media Landscape 2013". www.fredcavazza.net/2013/04/17/social-media-landscape-2013.

[6] Gupta, R. and Brooks, H. [Using Social Media for Global Security] John Wiley and Sons, Inc., Indianapolis, 34-39 (2013).

[7] Russom, P., "Big Data Analytics," TDWI Best Practices Report, 4th Quarter, 2011. tdwi.org/research/list/tdwi-best-practices-reports.aspx.

[8] Wang, Z., "Social Media Data Analysis: A Dynamic Perspective," NATO Technical Report RTO-MP-HFM-201 – Social Media: Risks and Opportunities in Military Applications, 28-1-28-10 (2012).

[9] Flynn, M.T. and Flynn, C.A., "Integrating Intelligence and Information: Ten Points for the Commander," Military Review 92(1), 4-8 (2012).

[10] Steele, R.D., "Open Source Intelligence".

[11] Servi, L., “Social Media Specialists Meeting Summary,” Human Social Culture Behavior Modeling Program Newsletter 13, 7-8 (2012). www.dtic.mil/biosys/files/HSCB-news-winter-2012.pdf.
[12] Gupta, R. and Brooks, H. [Social Media for Global Security], 47.
[13] Moon, W. (2009). “*Worldview – Subjective Reality – Threat Narrative: The Macro View*”. Working paper.
[14] Gupta, R. and Brooks, H. [Social Media for Global Security], 63-67.
[15] Shellman, S.M. and Levey, B., “Cascading Air Power Effects Simulation,” AFRL-RH-WP-TR-2011-0046 (2011).
[16] Fenstermacher, L., Kuznar, L., Yager, M., “Analysis of Discourse for Indications and Warnings,” Proceedings 2nd International Conference on Cross-Cultural Decision Making - 21-25 July 2012, 7307-7316 (2012).
[17] Shellman, S.M., “Leaders & their motivations: Explaining Government-Dissident Conflict-Cooperation Processes,” Conflict Management & Peace Science 23(1), 73–90 (2006).
[18] Shellman, S.M., “Process Matters: Conflict & Cooperation in Sequential Government-Dissident Interactions,” Security Studies 15(4), 563–99 (2006).
[19] Shellman, S.M., "Coding Disaggregated Intrastate Conflict: Machine Processing the Behavior of Substate Actors Over Time and Space," Political Analysis 16(4), 464-77 (2008).
[20] O’Brien, S., Shellman, S. and Covington, M., “Automated Discourse Analysis,” AFRL-RH-WP-TR-2013-0036.
[21] Lyon, E. and Afergan, B., “Social Media Conference Summary,” Human Social Culture Behavior Modeling Program Newsletter 13, 6-7 (2012). www.dtic.mil/biosys/files/HSCB-news-winter-2012.pdf.
[22] Charon, J.M., [The Meaning of Sociology], Prentice Hall, New Jersey (1992).
[23] Toman, P., Kuznar, L., Baker, T., et. al., “Analysis of Discursive Accent and Discursive Practices I&W”, AFRL-RH-WP-TR-2010-0128 (2010).
[24] Suedfeld, P., and Tetlock, P., “Integrative Complexity of Communications in International Crises,” The Journal of Conflict Resolution 21 (1), 169-184 (1977).
[25] Yonas, G., “The New Intelligence Organization,” News and Views 7(1), 1 (2005).

SPIE. DSS DEFENSE+ SECURITY

Issues and Challenges of Information Fusion in Contested Environments:

Autonomy, heterogeneity, and collaboration in contested environments

Georgiy Levchuk, Aptima Inc.

May 5th, 2014

APTIMA Human-Centered Engineering

SPIE. DSS DEFENSE+ SECURITY

Contested environments

APTIMA Human-Centered Engineering

- "Permissive" environments
  - Full establishment of air superiority
  - Examples: Afghanistan, Iraq
- "Contested" environments
  - Operate under jamming, advanced anti-aircraft weaponry, limited bandwidth
  - Needs: stealth, unmanned systems with high autonomy, low cost, limited communication
  - Examples: near-peer nations
- "Denied" environments
  - Limited or no aerial surveillance
  - Examples: China, Russia

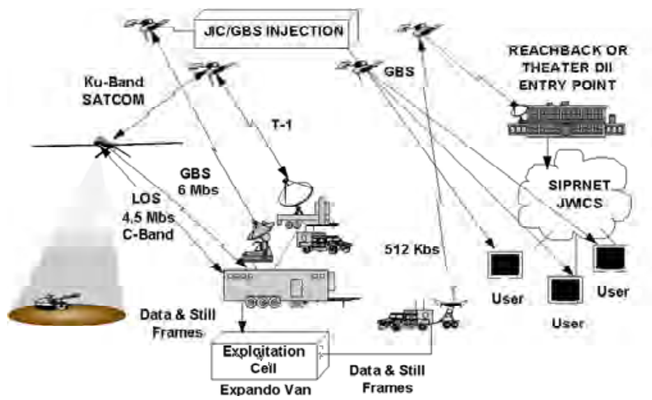
2

SPIE. DSS DEFENSE+ SECURITY

What is a problem?

APTIMA Human-Centered Engineering

- Traditional communication is via SATCOM or LOS
  - Raw data (e.g., FMV) communications result in high transmission rates
  - Easy to detect by enemy SIGINT
- Large platforms are too expensive



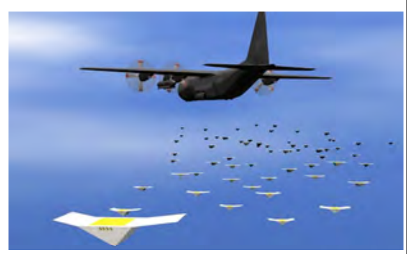
 3

SPIE. DSS DEFENSE+ SECURITY

What are possible solutions?

APTIMA Human-Centered Engineering

- Low-cost small heterogeneous ISR assets
  - Instead of large platforms capable of capturing many kinds of data, have small platforms with specific sensing capabilities
- Higher autonomy
  - Minimize the communication for control of the aircraft
- On-platform processing
  - Avoid communicating raw data
  - Perform processing at the platform instead of data center(s)



Large number of small sensor drones

Small-size and low-cost drone sensor

 4

Challenges in contested environments

- Planning and control
  - How to manage the employment of multiple sensors
  - Which sensors should be selected given their heterogeneous capabilities and the needs for other missions? How much autonomy can be given to different platforms?
  - If we allow high autonomy to the platforms, how can they avoid competition and achieve joint goals?
  - How can we deal with platform failures?
- Communication and collaboration
  - How can the platforms and sensors operate in communication-constrained environments?
  - How to make the assets communicate less while successfully achieve a joint mission
- Situation reconstruction
  - How to fuse the data from multiple assets to reconstruct a common picture

SPIE. DSS DEFENSE+ SECURITY
APTIMA Human-Centered Engineering

Communication and collaboration in contested environments

© 2013 Aptima, Inc.

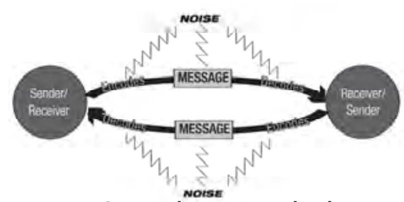
SPIE. DSS DEFENSE+ SECURITY

Collaboration and communication

APTIMA Human-Centered Engineering

- How should heterogeneous sensors communicate?
  – Stealthy
  – Limit communication volume
- What data should they transmit?
  – Only data relevant to receiver
- Analogy?
  – Human interactions
  – Influence operations

Linear communication

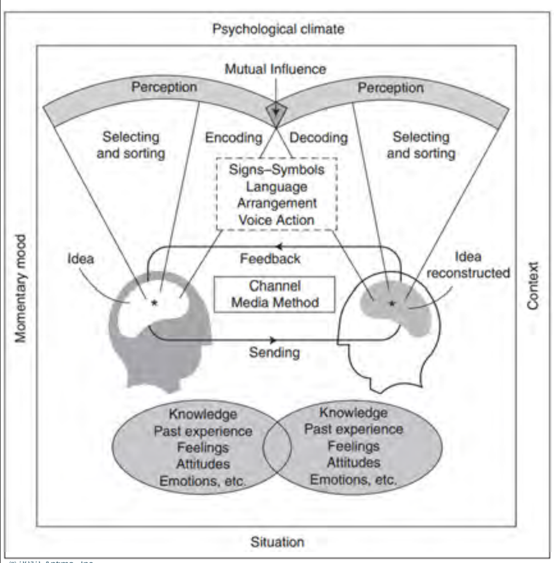


Interactive communication

SPIE. DSS DEFENSE+ SECURITY

The Ross communication model

APTIMA Human-Centered Engineering



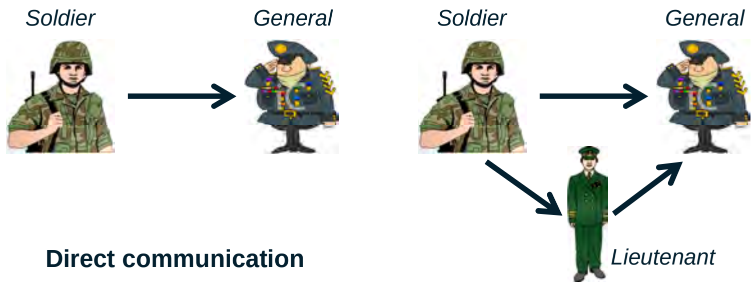
- Humans communicate *ideas* using **stories** to help receivers correctly reconstruct the ideas
  – This is not needed for controlled systems, like ISR networks, where the idea reconstruction can be encoded into the operation of the specific platform
- Humans have only perceptions of the need of the idea by receivers, while controlled resources can be given the knowledge of the general need for the idea/information
- Humans also engage in interactive communication, asking questions, which can be encoded as information seeking actions

SPIE. DSS DEFENSE+ SECURITY

Information-theoretic view of communication

APTIMA Human-Centered Engineering

- The message transmitted from soldier to general will have a different impact than the same message transmitted across multiple channels (also through a Lieutenant)
- This is an effect of fusing and decoding the information from multiple sources



Direct communication

Multi-channel communication

SPIE. DSS DEFENSE+ SECURITY

"Influence" operations

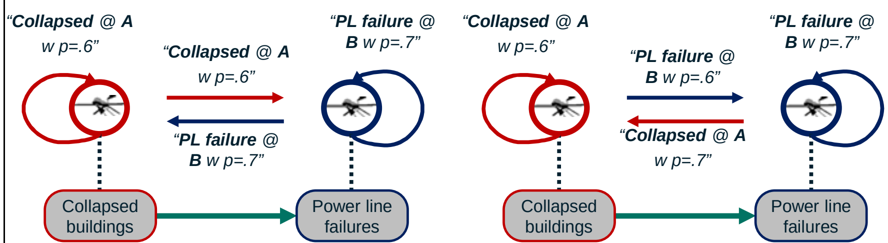
APTIMA Human-Centered Engineering

- Need fast reaction times
- Do not try to communicate facts
- Form the context and opinions of the receiver
- Influence receivers to accept particular views of the state of the world
- **Influence** the receivers to act
- Enabled by deep understanding of receiver's ***mental models***
  - Not needed for machines

How can "influence ops" be applied to distributed collaborative ISR?

SPIE. DSS DEFENSE+ SECURITY — APTIMA Human-Centered Engineering

- Example:
  - Disaster relief mission
  - Find locations of **collapsed buildings** and **electrical power line failures**
  - These locations spatially interdependent
- Traditional distributed processing:
  - Redundant communications, complex data fusion/integration at local node



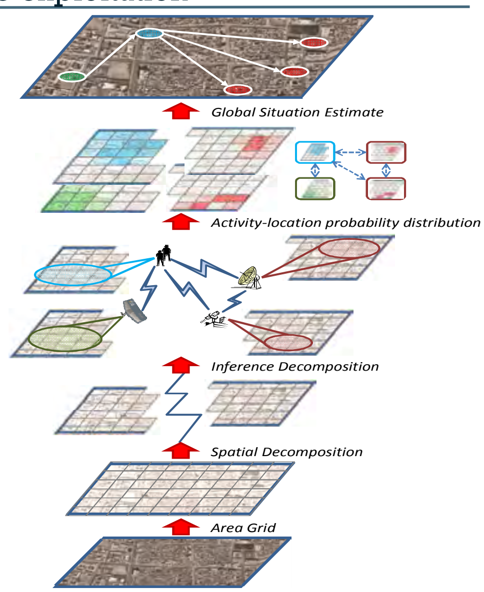
Traditional distributed exploitation **Influence-based exploitation**

 11

Operating in contested environments via collaborative exploitation

SPIE. DSS DEFENSE+ SECURITY — APTIMA Human-Centered Engineering

- Split the tasks geographically or functionally based on the asset's capabilities
- Platforms perform distributed search/actions and collaborate to synch their operations
- Information fusion is needed to allow individual assets to understand each other and generate "influence" messages



Conclusions about distributed ops in contested environments

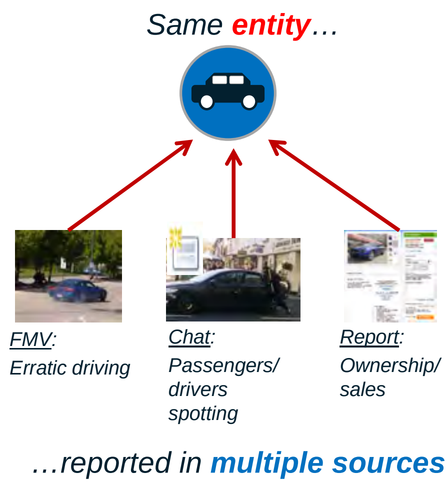
- Communication and collaboration in contested environments must combine
  - The encoding of the idea as messages over multiple channels
  - Communicating only the messages to influence the receivers
  - Prioritizing the communicated information based on impact, trading off the impact and the communication availability
- There is a principled communication model emerging based on "belief propagation"
  - The global problem can be decomposed into interdependent tasks (based on what needs to be done or found) and assigned to individual assets
  - The assets (agents) then operate on their local beliefs about the solution to individual tasks
  - The assets communicate beliefs that directly influence receiver's local beliefs

13

Situation reconstruction in contested environments

Information fusion

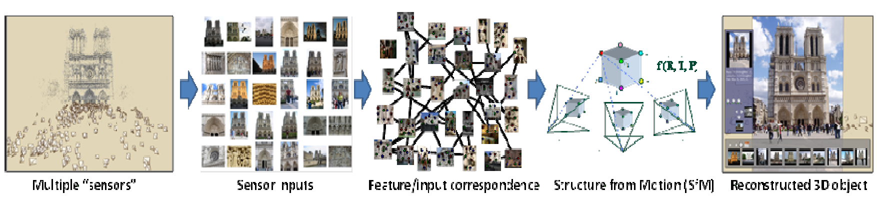
- Q: What is "information fusion"?
- A: Combining information about the same "**entity**" from **multiple sources** to increase quality of inferences/ assessments/ predictions/decisions
- Problem: **do not know that the entities reported in different sources are the same**
- Complication: **how can we resolve this in distributed manner?**



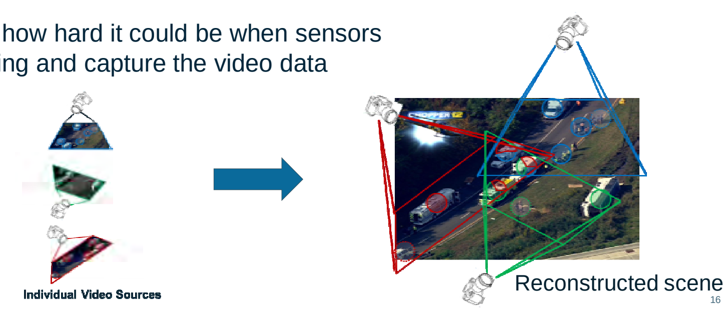
 15

Situation reconstruction from multiple heterogeneous sources-1

- Difficult even for homogeneous imagery sensors & stationary cameras



- Imagine how hard it could be when sensors are moving and capture the video data



 16

Situation reconstruction from multiple heterogeneous sources-2

SPIE. DSS DEFENSE+ SECURITY — APTIMA Human-Centered Engineering

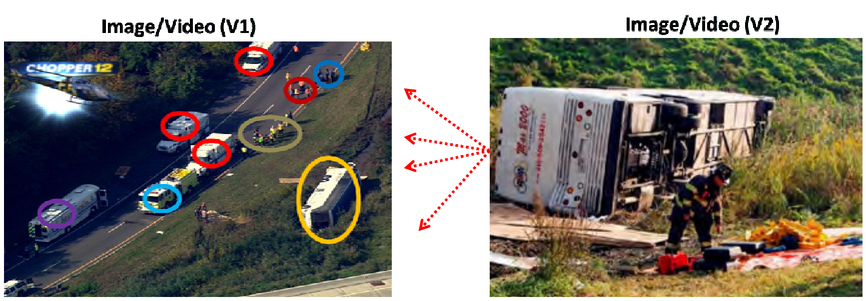
- Even harder to reconstruct the situation from diverse sensors

 17

What are challenges of multi-modal multi-source fusion?

SPIE. DSS DEFENSE+ SECURITY — APTIMA Human-Centered Engineering

- Overlap in the data
  - Reporting of the same entities/events by different sources
- Data at different levels of granularity
- Diverse and ambiguous appearance and semantics
- Can be addressed by **entity association/co-reference**
  - Easier with geographic locations, organizations, and people
  - Much harder with general activities and events
  - Entities, and especially events, in different sources do not have "global IDs"



Which vehicle is it?

 18

lxxiii

Other examples of entity/event/location association

SPIE. DSS DEFENSE+ SECURITY — APTIMA Human-Centered Engineering

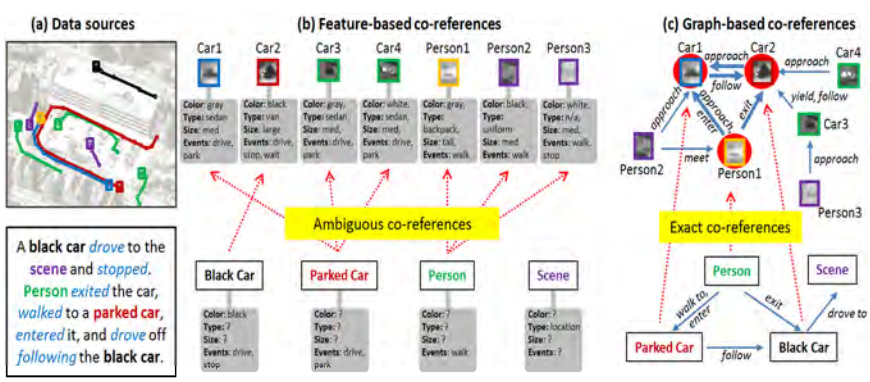
- This problem is particularly hard for sensors of different modalities and knowledge at different levels of information
- Example from Haiti “disaster relief” mission:

 19

Co-reference must incorporate context

SPIE. DSS DEFENSE+ SECURITY — APTIMA Human-Centered Engineering

- Incorporating not only features but relationships is critical for accurate co-reference
  – Allows to solve both association and classification problems simultaneously



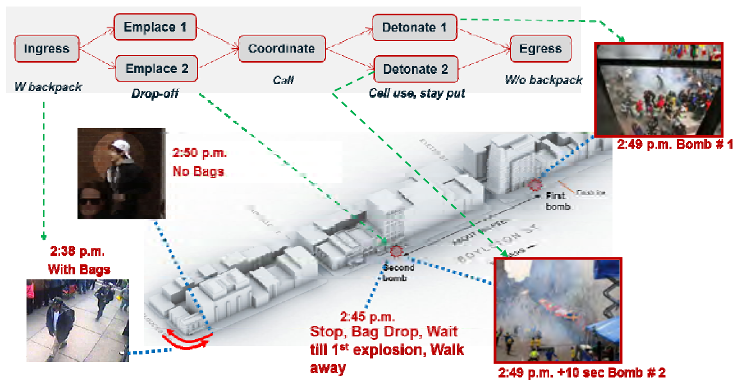
 20

SPIE. DSS DEFENSE+ SECURITY

Situation reconstruction in "denied environments"

APTIMA Human-Centered Engineering

- Given multiple data sources:
  - News media & Cellphone & Security camera images/video
  - Interviews/social media
- Reconstruct the locations, participants, and timing of events



 21

SPIE. DSS DEFENSE+ SECURITY

Conclusions

APTIMA Human-Centered Engineering

- Contested environments require low-cost low-exposure sensors and platforms
- Their autonomy must be maximized, while communications minimized
- Optimized cooperation between multiple heterogeneous assets can be achieved using collaborative belief-based communications not unlike how the humans exchange the knowledge
  - But with emphasis on "influence"
- Situation reconstruction from diverse sources requires common knowledge representation (e.g., aka human language) and entity association (co-reference)
  - Must be part of collaborative communications among distributed assets

 22

Autonomy, heterogeneity, and collaboration in contested environments

Georgiy Levchuk

Aptima Inc., 12 Gill Street, Suite 1400, Woburn, MA, USA 01801;

ABSTRACT

To operate in contested environments, the U.S. Military are changing the Intelligence, Surveillance, and Reconnaissance (ISR) operations by establishing a new fleet of autonomous sensors [1]. To be successful, these sensors must have low cost to reduce the sensitivity of sensor loss, high autonomy to operate when the communications are disrupted, on-board processing to avoid communicating large amounts of data to the ground processing centers, and collaborative policies to attain faster mission success in distributed manner without centralized control. These capabilities can be achieved if we change the concept of sensor collaboration from reporting collected data or local situation assessment to the communication using *influencing messages*. These messages represent how each sensor may influence other's local actions, and can be employed in joint reconstruction of the state of the environment by the fleet of heterogeneous sensors. Information fusion models for multi-modal relational data can assist in developing corresponding policies for collaborative distributed control and situation assessment.

Keywords: Distributed collaborative search, Contested environments, Information fusion, Mission autonomy, Situation reconstruction

1. NEW REQUIREMENTS FOR CONTESTED ENVIRONMENTS

Amounts of data that need to be collected, examined and shared during Intelligence, Surveillance, and Reconnaissance (ISR) operations are growing fast due to increasing sensor use. Most of current aerial ISR operations involve large multi-capable sensor platforms and rely on presence of unlimited communication. In contested environments, however, satellite (SATCOM) and line of sight (LOS) communications, which are the basis of most traditional ISR deployments (Figure 1 [2]), can be detected by adversaries' signals intelligence. As the result, large sensor platforms like Predator and Reaper UAVs may be easy targets of the anti-air defenses, and the loss of these expensive systems would be hard to sustain. In addition, the enemy may employ jamming technologies, making communication links intermittently disrupted. This will result in loss of control of remotely piloted systems, and inability to stream large volumes of high-resolution full motion video (FMV) to the ground exploitation centers. Instead of large expensive platforms capable of capturing many kinds of data, the new ISR force will include large number of small low-cost platforms with specific sensing capabilities. These sensors need to have high autonomy and on-board processing to reduce communication requirements. However, to attain fast mission execution and avoid competition, these platforms require efficient collaboration policies.

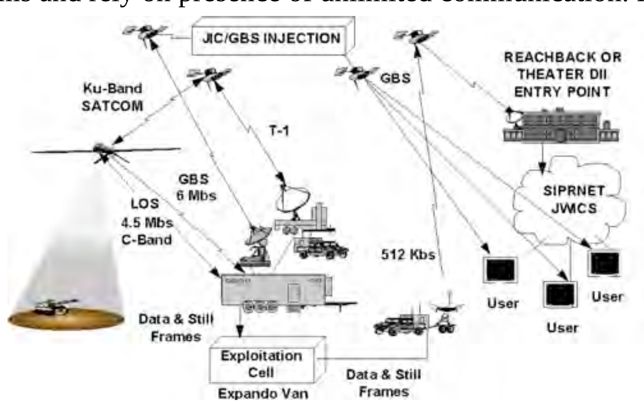


Figure 1 – Example of ISR communications: 1996 predator EUCOM deployment C^4I architecture

2. EFFECTIVE DISTRIBUTED COLLABORATION VIA BELIEF MESSAGES

Recently, distributed sensing and data processing has received significant attention in both research and development [3],[4] and acquisition programs. Most existing technologies were developed for raw data processing (e.g., detection of objects in imagery based on networks of cameras [5]), sensor placement [6], or coordinated planning and scheduling of homogeneous agents [7]. These solutions are inadequate for the general collaborative exploitation problems, since new ISR fleet will need to include multiple sensor modalities, heterogeneous computation capabilities, and may contain overlapping or complementary geographic regions or sensing tasks and targets.

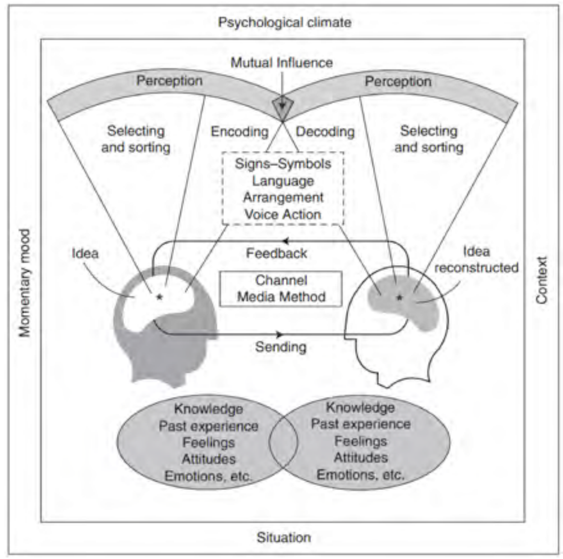


Figure 2 – ROSS model of communication

We pose that efficient and robust collaboration framework between autonomous systems can be developed following human communication models such as ROSS (Figure 2) [8] which encodes how the messages received from the senders are reconstructed based on the context and perceptual primitives of the receiver. Yet, there are specific differences between the humans and machines that can be used. Humans communicate using stories to help receivers correctly reconstruct the communicated ideas. This is not needed for controlled systems, like ISR sensor networks, where the idea reconstruction can be encoded into the operation of the specific platform. Also, humans may have perceptions of relevancies of their experience by other humans, while controlled platforms can be given the specific knowledge of requirements for the information by other platforms. Accordingly, the idea reconstruction can be performed at the sender rather than receiver, and the platforms can have shared mental models to facilitate this process. Humans also engage in interactive communication, asking questions, which can be encoded as information seeking actions

Such collaboration policy can be designed using the influence messages, which are the form of *belief distributions* of the location of collection targets or association of the information requests and the elements in the data [9]. Belief messages can be generated in distributed manner by the sensor logical units that are aware of the ISR mission given to the sensor fleet. Over the last decade the use of the belief-based collaboration policy have been successfully applied to communication and coordination in sensor networks [10],[11],[12].

The collaboration based on belief messages avoids the need to communicate the full experiences of the sensor platforms (Figure 3); the influence messages are more compact because the influence construction process exploits the dependencies between capabilities of sensors and their local ISR tasks. These tasks can be derived based on Essential Elements of Information (EEIs) that are defined based on commander's Priority Information Requirements (PIRs) [13], and the

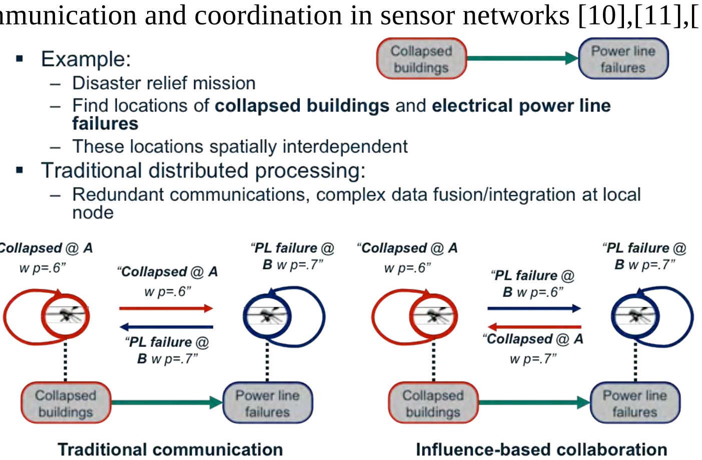


Figure 3 – Differences between traditional communication and influence-based collaboration

allocation of the ISR tasks to the sensors as well as distributed sensor C2 structure can be designed based on sensor capabilities for local computations, expected geographic information, and approximate communication constraints.

3. ENTITY ASSOCIATION IN DISTRIBUTED SCENE RECONSTRUCTION

The collections from a network of sensors may include data that overlaps in space and time. To avoid duplications during the reconstruction of environment (Figure 4), the *entity association* must be performed, where the entities can be landmarks, moving and static objects in the environments, events, activities, etc. Due to the lack of visual or auditory biometrics of the entities, the exact associations may be inaccurate. While the relational information may increase association accuracy [14], we pose that making hard association decisions may result in large inaccuracies in the situation assessments. Consequently, the situation reconstruction process must maintain and update uncertainties in the association between entities in different sensor feeds, and solve jointly the distributed reconstruction, association, and search problems.

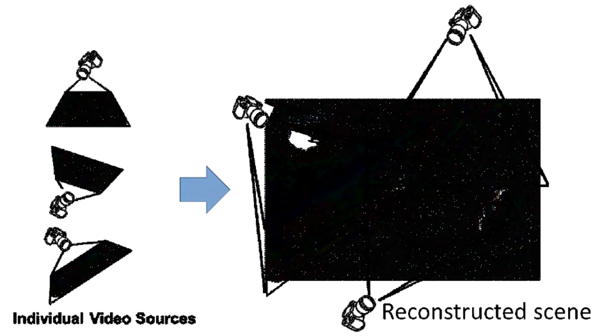


Figure 4 – Situation reconstruction from multiple video sources

4. CONCLUSIONS

Contested environments require low-cost low-exposure sensors and platforms which possess high autonomy and can adaptively reduce communication without degrading the mission performance. This can be achieved using collaborative belief-based communications not unlike how the humans exchange the knowledge when they attempt to influence one another. Situation reconstruction from diverse sources requires common knowledge representation (e.g., aka human language) and entity association (co-reference), which are maintained and updated at different levels of granularity.

REFERENCES

[1] Mehta, A. (2013) "General: DoD Needs ISR Fleet for Contested Environments", retrieved from: http://www.defensenews.com/article/20130918/DEFREG02/309180019/General-DoD-Needs-ISR-Fleet-Contested-Environments

[2] Dempsey, M. (2014) “Joint Concept for Entry Operations”, retrieved from: https://www.fas.org/irp/program/collect/docs/97-0230D.pdf

[3] Bryant, M., Johnson, P., Kent, B. M., Nowak, M., & Rogers, S. (2008). Layered sensing: its definition, attributes, and guiding principles for afrl strategic technology development. Wright-Patterson Air Force Base, Ohio: Sensors Directorate, Air Force Research Laboratory

[4] Dahm, W. (2010, 15 May). Technology Horizons: A Vision for Air Force Science and Technology During 2010-2030. Vol. 1, AF/ST-TR-10-01-PR.

[5] Ding, C., Song, B., Morye, A., Farrell, J. A., & Roy-Chowdhury, A. K. (2012). Collaborative sensing in a distributed PTZ camera network. Image Processing, IEEE Transactions on, 21(7), 3282-3295.

[6] Mathew, G., Surana, A., & Mezic, I. (2010). Uniform Coverage Control of Mobile Sensor Networks for Dynamic Target Detection. In Proceedings of the 49th IEEE Conference on Decision and Control, Atlanta, 2010

[7] Chen, W., Levy, R., & Decker, K. (2007) An Integrated Multi-Agent Coordination Including Planning, Scheduling, and Task Execution. Proceedings of the Workshop of Coordinating Agent's Planning and Scheduling (CAPS) at the Sixth AAMAS, Hawaii, USA

[8] “Introduction to Human Communication”, retrieved from: http://www.bvtpublishing.com/files/BV20Chapter01.pdf

[9] Levchuk, G., A. Ortiz, X. Yan, and J. Colonna-Romano, "Analysis of large-scale distributed knowledge sources via autonomous cooperative graph mining", to appear in Proceedings of SPIE DSS, 2014

[10] Crick, C., and A. Pfeffer (2003) Loopy Belief Propagation as a Basis for Communication in Sensor Networks, UAI, pp. 159-166

[11] Anker, T., D. Dolev, and B. Hodd (2008) Belief Propagation in Wireless Sensor Networks - A Practical Approach, Proceedings of the 3rd International Conference on Wireless Algorithms, Systems, and Applications, 466 – 479

[12] Rogers, A., Farinelli, A., Stranders, R., & Jennings, N. R. (2011). Bounded approximate decentralised coordination via the max-sum algorithm. Artificial Intelligence, 175(2), 730-759

[13] Levchuk, G., and K. Pattipati (2013) "Design of Distributed Command and Control for Collaborative Situation Assessment", Proceedings of ICCRTS

[14] Levchuk, G., and C. Shabarekh (2013) "Fusing video and text data via integrated appearance and behavior similarity", Proceedings of SPIE DSS