Office of the Secretary Of Defense (OSD)
Director of Defense Research & Engineering
Research Directorate
Small Business Innovation Research (SBIR)
FY2010.2 Program Description

Introduction

The OSD Director of Defense Research & Engineering (Research Directorate) SBIR Program is sponsoring topics in the following technology themes: Anti-Tamper (AT) Technology; Cognitive Readiness Technology; Energy and Power Technology; Human, Social, Cultural & Behavioral (HSCB) – Decision Support Tools Technology; Information Assurance – Cyber Conflict Defense Technology; and Large Data Handling Technology in this solicitation.

The Army, Navy, Air Force and DARPA are participating in the OSD SBIR Program on this solicitation. The service laboratories act as our OSD Agent in the management and execution of the contracts with small businesses. The service laboratories, often referred to as a DoD Component acting on behalf of the OSD, invite small business firms to submit proposals under this Small Business Innovation Research (SBIR) Program solicitation. In order to participate in the OSD SBIR Program this year, all potential proposers should register on the DoD SBIR Web site as soon as you can, and should follow the instruction for electronic submittal of proposals. It is required that all bidders submit their proposal cover sheet, company commercialization report and their firm's technical and cost proposal form electronically through the DoD SBIR/STTR Proposal Submission Web site at http://www.dodsbir.net/submission. If you experience problems submitting your proposal, call the help desk (toll free) at 1-866-724-7457. You must include a Company Commercialization Report as part of each proposal you submit; however, it does not count against the proposal page limit of 25 pages. Please note that improper handling of this form may result in the proposal being substantially delayed. Information provided may have a direct impact on the review of the proposal. The DoD SBIR Proposal Submission Web site allows your company to come in any time (prior to the proposal submission deadline) to edit your Cover Sheets, Technical and Cost Proposal and Company Commercialization Report.

We WILL NOT accept any proposals that are not submitted through the on-line submission site. The submission site does not limit the overall file size for each electronic proposal; there is only a 25-page limit. However, file uploads may take a great deal of time depending on your file size and your internet server connection speed. If you wish to upload a very large file, it is highly recommended that you submit prior to the deadline submittal date, as the last day is heavily trafficked. You are responsible for performing a virus check on each technical proposal file to be uploaded electronically. The detection of a virus on any submission may be cause for the rejection of the proposal. We will not accept e-mail submissions.

Firms with strong research and development capabilities in science or engineering in any of the topic areas described in this section and with the ability to commercialize the results are encouraged to participate. Subject to availability of funds, the DUSD(S&T) SBIR Program will support high quality research and development proposals of innovative concepts to solve the listed defense-related scientific or engineering problems, especially those concepts that also have high potential for commercialization in the private sector. Objectives of the DUSD(S&T) SBIR Program include stimulating technological innovation, strengthening the role of small business in meeting DoD research and development needs, fostering and encouraging participation by minority and disadvantaged persons in technological innovation, and increasing the commercial application of DoD-supported research and development

results. The guidelines presented in the solicitation incorporate and exploit the flexibility of the SBA Policy Directive to encourage proposals based on scientific and technical approaches most likely to yield results important to DoD and the private sector.

Description of the OSD SBIR Three Phase Program

Phase I is to determine, insofar as possible, the scientific or technical merit and feasibility of ideas submitted under the SBIR Program and will typically be one half-person year effort over a period not to exceed six months, with a dollar value up to $100,000. We plan to fund 3 Phase I contracts, on average, and down-select to one Phase II contract per topic. This is assuming that the proposals are sufficient in quality to fund this many. Proposals are evaluated using the Phase I evaluation criteria, in accordance with paragraph 4.2 of the DoD Solicitation Preface. Proposals should concentrate on that research and development which will significantly contribute to proving the scientific and technical feasibility of the proposed effort, the successful completion of which is a prerequisite for further DoD support in Phase II. The measure of Phase I success includes technical performance toward the topic objectives and evaluations of the extent to which Phase II results would have the potential to yield a product or process of continuing importance to DoD and the private sector, in accordance with Section 4.3.

Subsequent Phase II awards will be made to firms on the basis of results from the Phase I effort and the scientific and technical merit of the Phase II proposal in addressing the goals and objectives described in the topic. Phase II awards will typically cover 2 to 5 person-years of effort over a period generally not to exceed 24 months (subject to negotiation). Phase II is the principal research and development effort and is expected to produce a well defined deliverable prototype or process. A more comprehensive proposal will be required for Phase II.

Under Phase III, the DoD may award non-SBIR funded follow-on contracts for products or processes, which meet the Component mission needs. This solicitation is designed, in part, to encourage the conversion of federally sponsored research and development innovation into private sector applications. The small business is expected to use non-federal capital to pursue private sector applications of the research and development.

This solicitation is for Phase I proposals only. Any proposal submitted under prior SBIR solicitations will not be considered under this solicitation; however, offerors who were not awarded a contract in response to a particular topic under prior SBIR solicitations are free to update or modify and submit the same or modified proposal if it is responsive to any of the topics listed in this section.

For Phase II, no separate solicitation will be issued and no unsolicited proposals will be accepted. Only those firms that were awarded Phase I contracts, and have successfully completed their Phase I efforts, will be invited to submit a Phase II proposal. Invitations to submit Phase II proposals will be released at or before the end of the Phase I period of performance. The decision to invite a Phase II proposal will be made based upon the success of the Phase I contract to meet the technical goals of the topic, as well as the overall merit based upon the criteria in section 4.3. DoD is not obligated to make any awards under Phase I, II, or III. DoD is not responsible for any money expended by the proposer before award of any contract. For specifics regarding the evaluation and award of Phase I or II contracts, please read the front section of this solicitation very carefully. Every Phase II proposal will be reviewed for overall merit based upon the criteria in section 4.3 of this solicitation, repeated below:

a. The soundness, technical merit, and innovation of the proposed approach and its incremental progress toward topic or subtopic solution.

b. The qualifications of the proposed principal/key investigators, supporting staff, and consultants. Qualifications include not only the ability to perform the research and development but also the ability to commercialize the results.
c. The potential for commercial (defense and private sector) application and the benefits expected to accrue from this commercialization.

In addition, the OSD SBIR Program has a Phase II Plus Program, which provides matching SBIR funds to expand an existing Phase II contract that attracts investment funds from a DoD acquisition program, a non-SBIR/non-STTR government program or Private sector investments. Phase II Plus allows for an existing Phase II OSD SBIR contract to be extended for up to one year per Phase II Plus application, to perform additional research and development. Phase II Plus matching funds will be provided on a one-for-one basis up to a maximum $500,000 of SBIR funds. All Phase II Plus awards are subject to acceptance, review, and selection of candidate projects, are subject to availability of funding, and successful negotiation and award of a Phase II Plus contract modification. The funds provided by the DoD acquisition program or a non-SBIR/non-STTR government program must be obligated on the OSD Phase II contract as a modification just prior to or concurrent with the OSD SBIR funds. Private sector funds must be deemed an "outside investor" which may include such entities as another company, or an investor. It does not include the owners or family members, or affiliates of the small business (13 CFR 121.103).

The Fast Track provisions in section 4.0 of this solicitation apply as follows. Under the Fast Track policy, SBIR projects that attract matching cash from an outside investor for their Phase II effort have an opportunity to receive interim funding between Phases I and II, to be evaluated for Phase II under an expedited process, and to be selected for Phase II award provided they meet or exceed the technical thresholds and have met their Phase I technical goals, as discussed Section 4.5. Under the Fast Track Program, a company submits a Fast Track application, including statement of work and cost estimate, within 120 to 180 days of the award of a Phase I contract (see the Fast Track Application Form on www.dodsbir.net/submission). Also submitted at this time is a commitment of third party funding for Phase II. Subsequently, the company must submit its Phase I Final Report and its Phase II proposal no later than 210 days after the effective date of Phase I, and must certify, within 45 days of being selected for Phase II award, that all matching funds have been transferred to the company. For projects that qualify for the Fast Track (as discussed in Section 4.5), DoD will evaluate the Phase II proposals in an expedited manner in accordance with the above criteria, and may select these proposals for Phase II award provided: (1) they meet or exceed selection criteria (a) and (b) above and (2) the project has substantially met its Phase I technical goals (and assuming budgetary and other programmatic factors are met, as discussed in Section 4.1). Fast Track proposals, having attracted matching cash from an outside investor, presumptively meet criterion (c). However, selection and award of a Fast Track proposal is not mandated and DoD retains the discretion not to select or fund any Fast Track proposal.

Follow-On Funding

In addition to supporting scientific and engineering research and development, another important goal of the program is conversion of DoD-supported research and development into commercial (both Defense and Private Sector) products. Proposers are encouraged to obtain a contingent commitment for follow-on funding prior to Phase II where it is felt that the research and development has commercialization potential in either a Defense system or the private sector. Proposers who feel that their research and development have the potential to meet Defense system objectives or private sector market needs are encouraged to obtain either non-SBIR DoD follow-on funding or non-federal follow-on funding, for Phase III to pursue commercialization development. The commitment should be obtained during the course of Phase I performance, or early in the Phase II performance. This commitment may be

contingent upon the DoD supported development meeting some specific technical objectives in Phase II which if met, would justify funding to pursue further development for commercial (either Defense related or private sector) purposes in Phase III. The recipient will be permitted to obtain commercial rights to any invention made in either Phase I or Phase II, subject to the patent policies stated elsewhere in this solicitation.

Contact with DoD

General informational questions pertaining to proposal instructions contained in this solicitation should be directed to the topic authors and point of contact identified in the topic description section. Proposals should be electronically submitted. Oral communications with DoD personnel regarding the technical content of this solicitation during the pre-solicitation phase are allowed, however, proposal evaluation is conducted only on the written submittal. Oral communications during the pre-solicitation period should be considered informal, and will not be factored into the selection for award of contracts. Oral communications subsequent to the pre-solicitation period, during the Phase I proposal preparation periods are prohibited for reasons of competitive fairness; however, to obtain answers to technical questions during the formal Solicitation period, please visit http://www.dodsbir.net/sitis. Refer to the front section of the solicitation for the exact dates.

Proposal Submission

Proposals shall be submitted in response to a specific topic identified in the following topic description sections. The topics listed are the only topics for which proposals will be accepted. Scientific and technical information assistance may be requested by using the SBIR/STTR Interactive Technical Information System (SITIS).

It is required that all bidders submit their proposal cover sheet, company commercialization report and their firm's technical and cost proposal form electronically through the DoD SBIR/STTR Proposal Submission Web site at http://www.dodsbir.net/submission. (This applies to both Phase I and Phase II proposal submission.) If you experience problems submitting your proposal, call the help desk (toll free) at 866-724-7457. You must include a Company Commercialization Report as part of each proposal you submit; however, it does not count against the proposal page limit of 25 pages. Please note that improper handling of this form may result in the proposal being substantially delayed. Information provided may have a direct impact on the review of the proposal. The proposal submission Web site allows your company to come in any time (prior to the proposal submission deadline) to edit your Cover Sheets, Technical and Cost Proposal and Company Commercialization Report. We **WILL NOT accept any proposals which are not submitted through the on-line submission site.** The submission site does not limit the overall file size for each electronic proposal, only the number of pages is limited. However, file uploads may take a great deal of time depending on your file size and your internet server connection speed. You are responsible for performing a virus check on each technical proposal file to be uploaded electronically. The detection of a virus on any submission may be cause for the rejection of the proposal. We will not accept e-mail submissions.

The following pages contain a summary of the technology focus areas, followed by the topics.

Anti-Tamper (AT) Technology Focus Area

DoD Anti-Tamper policy directives outline requirements to provide anti-tamper protection to Critical Program Information (CPI) on all new start programs, all pre-planned product improvement or technology insertion efforts, and FMS/DCS programs. Although significant advances have been made in a number of enabling technologies for Anti-Tamper, such as protective materials, microelectronics, and software protection techniques, significant technical challenges remain to address the full scope of the exploitation threat. Studies indicate that approximately 80% of all CPI is contained in software/firmware. A broader range of robust techniques or technologies that protect software, data, and firmware is essential and will have a broad impact on protecting CPI. Secure programmable logic devices and secure processors are needed. Improvements are needed in existing protective coating technologies in order to reduce the impact on system reliability. The ability to detect the wide range of potential tamper events requires new and innovative approaches to tamper sensor technology. Finally, power solutions that would provide primary or secondary latent power for tamper sensors and responses are needed.

This focus area includes: development of protection techniques against reverse engineering of Electro-Optical detectors and Optical components; development of a practical physical unclonable function with higher entropy for use in a field programmable gate array; new innovative technology or techniques to verify that a system's configuration matches the intended baseline configuration as a normal part of its startup routine, in order to detect system modification or tampering; research and development of technology, tools, and/or fabrication/design guidelines and methods to prevent, identify, or severely limit reverse engineering techniques on microelectronic devices; development of a tamper resistant, multiprocessor, embedded computer system architecture consisting of a microprocessor, a digital signal processor, field programmable gate array and graphics processing unit technology; research the existence, detection and analysis of an electromagnetic field radiated during FPGA bit stream operation; Development of innovative trusted intellectual property (circuit designs, embeddable micro-code, and the like) that will prevent other portions of an integrated circuit or field programmable gate array design from operating in modes, malicious or accidental, other than those intended by the designer; make possible trusted intellectual property in untrusted fabrication environments through the development of methods and designs that allows the determination that no unintended functionality has been added to a hardware device in the time between when the design is provided to the foundry and when the finished device is provided to the user; development of zero power/ultra low power tampering/reverse engineering sensor technology for use at the printed circuit board level, or integrated circuit level, including sensor, material, or techniques capable of mitigating the effectiveness of nondestructive probing by an exploiter seeking to conduct localized buried structure analysis.

The Anti-Tamper (AT) Technology topics are:

OSD10-A01	EO/Optical Protection
OSD10-A02	Field Programmable Gate Array (FPGA) Physical Unclonable Functions
OSD10-A03	System Configuration Verification
OSD10-A04	Anti-Reverse Engineering (RE) Techniques
OSD10-A05	Tamper Resistant UAV/UGV Embedded Architecture
OSD10-A06	FPGA Bit Stream Data Electromagnetic Field Analysis
OSD10-A07	Incorporation of Trust into Integrated Circuit (IC) and Field Programmable Gate Array (FPGA) Design
OSD10-A08	Intellectual Property (IP) in Untrusted Fabrication Environments
OSD10-A09	Zero Power/Ultra Low Power Tamper Detection Sensors

Cognitive Readiness Technology Focus Area:

Cognitive readiness is the mental preparation (including skills, knowledge, abilities, motivations, and personal dispositions) an individual needs to establish and sustain competent performance in the complex and unpredictable environment of modern military operations. Cognitive readiness may be understood as a combination of three basic abilities: 1) Recognize new situational patterns in the battle space (requiring adjustments in situation awareness, new knowledge, and transfer of training); 2) modify problem solutions associated with these patterns as required by the current situation (requiring adjustments in meta-cognition, socio-cultural agility, and creativity); and, 3) design and implementation of plans of action based on these solutions (requiring adjustments to decision-making, leadership, and controlling emotions in new social environments).

This theme supports research that will utilize the knowledge products from disciplines such as cognitive science, network science, augmented cognition, neuroergonomics, learning science, psychology, and sociology to pioneer new developments to enable the cognitive readiness of warfighters. This theme supports research, such as serious game environments, that can be used to develop relevant models and to push the envelope on providing new analysis, decision support, and training capabilities in social, cultural and language domains for the deployed warfighter in organizational echelons from combat teams to Joint Task Force Headquarters. A focus of this technology is developing unique and operationally relevant models and content. Topics seek validated socio-cultural models and content with demonstrated use-case effectiveness. They seek to provide the interactive, dynamic environments that would support better cultural awareness. The technologies should be extensible beyond current operations in Iraq and Afghanistan to other regions and military kinetic and non-kinetic scenarios. Networkable, remote-capable products are desirable with emphasis on insertion into systems of record and Just In Time training environments. Training related topics require SCORM compliance and the adoption of existing /emerging standards for training of language and cultural skills.

The Cognitive Readiness Technology topics are:

OSD10-CR1	Rapid Assessment of Team Cognitive Readiness
OSD10-CR2	Neuro Cognitive Control of Human Machine Systems
OSD10-CR3	Immersive Scenario Based Training Environments for Intuitive Decision Making
OSD10-CR4	Training Battery for the Rapid Formation of Cognitively Ready, Effective Teams
OSD10-CR5	Generation of the Army Cognitive Readiness Assessment (ACRA)
OSD10-CR6	Distributed Team Workload Assessment Tool
OSD10-CR7	Improving Team Readiness through the Convergence of Team Mental Models
OSD10-CR8	Decision Support: Cognitive Readiness Assessment and Reporting
OSD10-CR9	Embeddable Agents for Assessing Cognitive Readiness
OSD10-C10	Real-time Cognitive Readiness Assessment Tool

Energy and Power Technology Focus Area

Technology advances in electric power generation, distribution, and use are enabling new, transformational military capabilities. Advanced energy and power technologies are providing the critical concepts, architectures, and systems to enable this revolutionary warfighting advantage. Integrating and distributing power on manned and unmanned ships, aircraft, ground vehicles and other platforms leads to significant enhancements in platform flexibility, survivability, lethality and effectiveness. The Army's transformation challenge is to develop a smaller, lighter, and faster force, utilizing hybrid electric drive, electric armament and protection, and a reduced logistical footprint. The Navy is developing future ships that integrate electric power into a next-generation architecture which enables directed energy weapons, electromagnetic launchers and recovery, new sensors, as well as supporting significant fuel, maintenance, and manning reductions. The Air Force needs electric power to replace complex mechanical, hydraulic and pneumatic subsystems, and also enable advanced electric armament systems. Improved batteries/power sources will support the individual soldier by permitting longer mission durations and reduced weight borne by the soldier. Space based operational capability improvements include a more electric architecture for responsive and affordable delivery of mission assets, and powering space based radar systems.

More electric and all-electric systems have distinct technological advantages but are coupled with inherent disadvantages – principally, the need for more power generation and a marked increase in waste heat generated by ever smaller electronic components. The use of solar power at forward operating bases reduces the need for supply convoys transporting batteries and liquid fuels into war zones. Quiet systems minimize risk of discovery during field operations. Warfighting capabilities are optimized when energy and power systems are quiet, efficient, lightweight, and easy to use, and require minimal logistical support.

The Energy and Power Technology topics are:

OSD10-EP1	Parallel Operation of Compact, Efficient Turbogenerators for Robust Tactical Energy Independence
OSD10-EP2	Rugged, collapsible solar concentration devices to support tactical alternative energy production
OSD10-EP3	APU Silencing Technology Development
OSD10-EP4	Near Field Contactless Electric Power Transfer
OSD10-EP5	Redeployable Solar Combined Heat and Power (RSCHP) System
OSD10-EP6	Anion Exchange Membranes for Alkaline and Low-temperature Fuel Cell Applications
OSD10-EP7	Advanced System-Level Integration for High Efficiency Primary and Secondary (Waste Heat) Thermoelectric Generation
OSD10-EP8	Magnetic Gears and Couplings

Human, Social, Cultural & Behavioral (HSCB) – Decision Support Tools Technology Focus Area

Current military operations need and future operations will demand the capability to understand the social and cultural terrain and the various dimensions of human behavior within those terrains. Behaviors in the social and cultural terrain context extend across the spectrum, from adversaries to our joint U.S. forces, with our coalition partners, and with government and non-government organizations. For operational, strategic and tactical warfighters, there is a significant need for socio-cultural models that provide predictive capabilities with regard to the behavior of adversaries and contested populations.

The Department of Defense is increasing the investment in "non-kinetic" capabilities, relative to the traditional "kinetic" capabilities of weapons platforms and munitions. A portion of this new investment strategy is focused on increasing awareness and understanding of the impact of cultural, social, and behavioral variables within the operational environment. Additionally, Irregular Warfare (IW) and the subsequent need of non-kinetic capabilities are a matter of strategic importance to the military, on par with our capability to wage traditional warfare.

DoD's HSCB technology area emphasizes the application of knowledge, skills, and supporting technologies to give the DoD the ability to understand the complex human terrain and socio-cultural environments in which we operate. This work merges the social and behavioral sciences with the computational and computer sciences to deliver the methodologies and tools to support Phase 0 (planning/shaping) to Phase 4 (stabilization) military operations critical to success in military operations (DDR&E Strategic Plan). OSD's HSCB modeling efforts are focused on narrowing the gap between social and behavioral science capabilities and military utility via the development of cross-domain capabilities and tools. Investment in enhanced HSCB modeling capabilities and tools requires the simultaneous development of decision support tools and systems that enable the end-user to make optimal use of HSCB model outputs and data.

The HSCB Technology topics are:

OSD10-HS1	Decision Superiority through Enhanced Cultural Intelligence Forecasting
OSD10-HS2	In Situ Collection of Human Social Cultural Behavioral Data
OSD10-HS3	Neuromorphic Models of Human Social Cultural Behavior (HSCB)
OSD10-HS4	Dynamic Meta-Network Measures
OSD10-HS5	Visualization Methods and Tools for Human, Social, Cultural, and Behavioral Models
OSD10-HS6	Automated Network Construction
OSD10-HS7	Analytical Tools for Local Economic Analysis
OSD10-HS8	An Adaptive Cultural Trainer for Development of Cultural Aptitude in Warfighters
OSD10-HS9	Developing and Modeling Social Networks inside Technology Poor Societies

Information Assurance – Cyber Conflict Defense Technology Focus Area

As the cyber threat continues to increase in sophistication and complexity, the DoD must be prepared to defend the ability to provide the information and processing needed to support critical missions during a cyber conflict. Networks and systems must be built with the ability to use alternate paths and survivable architectures and algorithms to get the critical work done even when attacked in unanticipated ways that may succeed in interfering with their normal operation. We also need to make it harder for a determined adversary to succeed against us, for instance, by increasing redundancy, diversity, and agility to disrupt attack planning. The DoD needs new tools and technologies to force capable adversaries to spend more, move more slowly, and take bigger risks, while providing mission assurance by enabling us to fight through cyber degradation. The DoD must go beyond efforts to build and maintain security in systems overwhelmingly built from commercial off-the-shelf technology. Hardening DOD networks will require key security components with high assurance and of known pedigree as well as adaptable and robust defenses.

As envisioned, the Global Information Grid (GIG) will connect the roughly 3 million computers, 100,000 LANs, 100 long distance networks, and a multitude of wireless networks and devices in support of all DoD. It will underlie the increased ability to conduct network-centric operations, providing the joint warfighter with a single, end-to-end information system capability, built on a secure, robust network-centric environment. It will allow users to post and access shared data and applications regardless of their location – while inhibiting or denying an adversary's ability to do the same – in a converged heterogeneous enterprise capable of protecting content of different sensitivities. DoD's unprecedented enterprise vision for future information operations must simultaneously address protecting and defending its critical information and information technology systems by ensuring availability, integrity, authentication, confidentiality and non-repudiation; and by providing security management and operations that incorporate the requisite protection, detection, and quick reaction capabilities.

Further, as operations are ever-more enmeshed in the decentralized fabric of the GIG, the converged, decentralized vision of the future network requires a parallel adoption of a decentralized trust paradigm. Degrees of trust and robustness hitherto provided by enclave isolation and separation must be distributed across the networks down to the tactical edge devices. DoD is making significant IA investments in ensuring the security of net-centric operations of the GIG. The scope of the challenges, the dynamics of the information technology industry, and the need for dynamically optimizing defenses within particular mission contexts provide multiple opportunities for new and innovative security solutions. In particular new technology solutions are needed for supporting the edge users who must operate across multiple domains and communications paths, on less hardened networks, to reach other tactical mission players, and to access protected core information systems and data warehouses.

The Information Assurance Technology topics are:

OSD10-IA1	Countermeasures to Malicious Hardware to Improve Software Protection Systems
OSD10-IA2	Effective Portable Data Content Inspection and Sanitization
OSD10-IA3	Robust and Efficient Anti-Phishing Techniques
OSD10-IA4	Preventing Sensitive Information and Malicious Traffic from Leaving Computers
OSD10-IA5	Biometric-based Computer Authentication During Mission Oriented Protective Posture Scenarios

Large Data Handling Technology Focus Area

As the Department of Defense increases the capability and capacity to generate increasing amounts of data from the numerous sensors in the battlespace, the issue of handling very large data sets has become more challenging. This is in part due to Department of Defense response to a changing threat environment where there is an expansion of the types of sensors deployed, new types of information collected, and different features used to classify these new threats. From a technical perspective, sensor processing speeds have outpaced the speed and ability to transport, store and process the data created.

Research in the areas of Architecture, Shaping Data for Exploitation, and Data Discovery for Exploitation are of interest. In addition to the research and development of technology and approaches, it is important to evaluate the impact of these efforts areas with regards to the way they change how large data sets are handled.

(a) Architectures – Both the size of the data to be transferred and the growing size of databases requires novel architectural approaches to provide the adaptability and usability (automation and performance impact of human in the loop). Current databases, file systems and network protocols will not keep pace.

(b) Shaping Sensor Data for Exploitation – When tracing the processing chain from multi-source sensor inputs to the user/analysts, the techniques that are known and used become fewer and less mature. The simple process chain view goes from (1) metadata tagging to (2) pre-processing to (3) multi-source common data representation to (4) triage/identify high priority data subsets for analysis and action. Candidate research areas include pattern analysis, data classification for importance and prioritization, criticality assessment, change detection, uncertainty management and reduction, high level structures, data search and retrieval, feature extraction, automatic translation, and automated or assisted pattern recognition.

(c) Data Discovery for Exploitation – In order to better to discover and exploit the growing amount of sensor data, the following areas of research are considered: Object recognition in scenes and streams, discovery and exploitation at the edge, structuring knowledge for discovery, improving analytic throughput, aiding ISR functions, layered analysis and interpretation, effects prediction for decision support and cross domain access for effective ISR

The Large Data Handling topics are:

OSD10-L01	Temporal and Conceptual Extractions of Complex Social Network Data
OSD10-L02	Multi-sensor Extraction for Social Network Analysis - Tactical
OSD10-L03	End to End Analysis of Information Architectures
OSD10-L04	Automated Scene Understanding
OSD10-L05	Shaping Sensor Data for Exploitation
OSD10-L06	Knowledge Discovery using Mobile Devices
OSD10-L07	Data Discovery for Exploitation from Distributed Sources
OSD10-L08	Real-time Resource Allocation Co-Processor
OSD10-L09	Framework for Large Streaming Data Analysis

OSD SBIR 10.2 Topic Index

OSD10-A01	EO/Optical Protection
OSD10-A02	Field Programmable Gate Array (FPGA) Physical Unclonable Functions
OSD10-A03	System Configuration Verification
OSD10-A04	Anti-Reverse Engineering (RE) Techniques
OSD10-A05	Tamper Resistant UAV/UGV Embedded Architecture
OSD10-A06	FPGA Bit Stream Data Electromagnetic Field Analysis
OSD10-A07	Incorporation of trust into integrated circuit (IC) and field programmable gate array (FPGA) design
OSD10-A08	Intellectual Property (IP) in untrusted fabrication environments
OSD10-A09	Zero Power/Ultra Low Power Tamper Detection Sensors
OSD10-CR1	Rapid Assessment of Team Cognitive Readiness
OSD10-CR2	Neuro Cognitive Control of Human Machine Systems
OSD10-CR3	Immersive Scenario Based Training Environments for Intuitive Decision Making
OSD10-CR4	Training Battery for the Rapid Formation of Cognitively Ready, Effective Teams
OSD10-CR5	Generation of the Army Cognitive Readiness Assessment (ACRA)
OSD10-CR6	Distributed Team Workload Assessment Tool
OSD10-CR7	Improving Team Readiness through the Convergence of Team Mental Models
OSD10-CR8	Decision Support: Cognitive Readiness Assessment and Reporting
OSD10-CR9	Embeddable Agents for Assessing Cognitive Readiness
OSD10-C10	Real-time Cognitive Readiness Assessment Tool
OSD10-EP1	Parallel Operation of Compact, Efficient Turbogenerators for Robust Tactical Energy Independence
OSD10-EP2	Rugged, collapsible solar concentration devices to support tactical alternative energy production
OSD10-EP3	APU Silencing Technology Development
OSD10-EP4	Near Field Contactless Electric Power Transfer
OSD10-EP5	Redeployable Solar Combined Heat and Power (RSCHP) System
OSD10-EP6	Anion Exchange Membranes for Alkaline and Low-temperature Fuel Cell Applications
OSD10-EP7	Advanced System-Level Integration for High Efficiency Primary and Secondary (Waste Heat) Thermoelectric Generation
OSD10-EP8	Magnetic Gears and Couplings
OSD10-HS1	Decision Superiority through Enhanced Cultural Intelligence Forecasting
OSD10-HS2	In Situ Collection of Human Social Cultural Behavioral Data
OSD10-HS3	Neuromorphic Models of Human Social Cultural Behavior (HSCB)
OSD10-HS4	Dynamic Meta-Network Analysis
OSD10-HS5	Visualization Methods and Tools for Human, Social, Cultural, and Behavioral Models
OSD10-HS6	Automated Network Construction
OSD10-HS7	Analytical Tools for Local Economic Analysis
OSD10-HS8	An Adaptive Cultural Trainer for Development of Cultural Aptitude in Warfighters
OSD10-HS9	Developing and Modeling Social Networks inside Technology Poor Societies
OSD10-IA1	Countermeasures to Malicious Hardware to Improve Software Protection Systems
OSD10-IA2	Effective portable data content inspection and sanitization
OSD10-IA3	Robust and Efficient Anti-Phishing Techniques
OSD10-IA4	Preventing Sensitive Information and Malicious Traffic from Leaving Computers
OSD10-IA5	Biometric-based Computer Authentication during Mission Oriented Protective Posture Scenarios
OSD10-L01	Temporal and Conceptual Extractions of Complex Social Network Data
OSD10-L02	Multi-sensor Extraction for Social Network Analysis - Tactical
OSD10-L03	End to End Analysis of Information Architectures
OSD10-L04	Automated Scene Understanding
OSD10-L05	Shaping Sensor Data for Exploitation
OSD10-L06	Knowledge Discovery using Mobile Devices
OSD10-L07	Data Discovery for Exploitation from Distributed Sources

OSD10-L08	Real-time Resource Allocation Co-Processor
OSD10-L09	Framework for Large Streaming Data Analysis

OSD SBIR 10.2 Topic Descriptions

OSD10-A01 TITLE: EO/Optical Protection

TECHNOLOGY AREAS: Materials/Processes, Sensors

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), which controls the export and import of defense-related material and services. Offerors must disclose any proposed use of foreign nationals, their country of origin, and what tasks each would accomplish in the statement of work in accordance with section 3.5.b.(7) of the solicitation.

OBJECTIVE: Develop protection techniques against reverse engineering of Electro-Optical detectors and Optical components. Electro-Optical detectors and Optical components used in various military sensors and military equipment have designs and components that contain critical technology. Some of the components include; IR Focal Plane Array (FPA), Intensifier tubes used in Night Vision Goggles (NVG) or NV equipment. This SBIR effort involves detection of and protection against reverse engineering attacks on the optical design, laser couplers, and optical limiters.

DESCRIPTION: Adversaries may attempt to reverse engineer electro-optical detectors, such as IR FPAs or intensifier tubes, and optical components, such as laser couplers and optical limiters, to copy critical technology or to determine methods of countering military systems. Approaches need to be investigated that would prevent technology capture through examination of the physical structure of these critical components, characterization of operating bandwidths, or identification of physical components. Protection of military sensors and equipment is sought using a combination of techniques, including: volume protection, tamper detection, and novel destruction methods. Participation in this SBIR is limited to US citizens and US persons.

PHASE I: Research the feasibility of developing protection capabilities for electro-optical and optical components. Protection approaches must not significantly degrade system performance. Simulations, simple prototypes, and/or models may be used to demonstrate the feasibility of protecting optical systems. Offerer will describe the reverse engineering attack that the proposed protection technology counters, and estimate the impact upon system performance. Submit a final report to the government describing the proposed protection technology.

PHASE II: Develop a prototype protection system for electro-optical or optical components based on the phase I research. An independent lab is to test and evaluate the protection technology. Provide a copy of the test and evaluation report to the government. Deliver to the government point of contact, two prototypes which are integrated in two components of interest for testing and evaluation. At the government's facility, provide a two day on site seminar covering the protection technology. Provide the government point of contact with a final report.

PHASE III DUAL USE APPLICATIONS:
Department of Defense Directive (DOD) 5000.2R provides instructions on identifying critical technologies and on defining methods to protect them. Commercialization opportunities exist throughout the Defense Department and within the government agencies such as the Department of Homeland Security and Intelligence Community for technologies to protect critical technologies. Applications for a commercial version of the technology include protecting fiber optic communication systems, and optical computer networks.

REFERENCES:
[1] D. Banks and C. Toumazou: "Reverse engineering the principal image processing architectures of the Macula Lutea within the human retina," pp. 237 – 240, Nov. 2008.

[2] A. Simoni, et al.: "Integrated optical sensors for 3-D vision," Proceedings of IEEE Sensors, Vol. 1, pp. 1–4, June 2002.

[3] E. Mei and D. Gallinger: "Optical system spectral transmission measurements in the visible and infrared," IEEE Automatic Testing Conference, pp. 242 – 248, Sept. 1989.

[4] W. Yong-gang, et al.: "High performance data acquisition system for IRFPA testing," IEEE International Symposium on Circuits and Systems, pp. 2649 – 2652, May 2008.

[5] T. Kelly, Jr.: "Advanced test equipment for third generation FLIRs," IEEE AUTOTESTCON Proceedings Systems Readiness Technology Conference, 263 – 270, Aug. 2001.

KEYWORDS: electro-optics, infrared, radio frequency, RF, protection, night vision, goggle, hardware, focal-plane array, FPA.

OSD10-A02 TITLE: Field Programmable Gate Array (FPGA) Physical Unclonable Functions

TECHNOLOGY AREAS: Information Systems, Materials/Processes

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), which controls the export and import of defense-related material and services. Offerors must disclose any proposed use of foreign nationals, their country of origin, and what tasks each would accomplish in the statement of work in accordance with section 3.5.b.(7) of the solicitation.

OBJECTIVE: Current physical unclonable functions (also called provable unclonable functions) have a relatively low entropy. Develop a practical physical unclonable function (PUF) with higher entropy for use in a field programmable gate array.

DESCRIPTION: Physical Unclonable Functions raise the security and trust of semiconductor ICs and IC based systems due to the unpredictable way they respond to an applied stimulus as in a challenge-response authentication. It is effectively impossible to clone PUF based ICs. PUFs do not store secret keys for cryptographic operations. PUFs dynamically generate a virtually unlimited number of unique, volatile secrets for each IC. PUFs are inherently tamper proof. An invasive physical attack will change the PUF characteristics, which prevent successful authentication and disable key generation applications. PUFs eliminate the need to store and manage cryptographic keys by securely generating new keys for every authentication event.

The goal of this research is to develop an improved field programmable gate array based physical unclonable function with a higher level of entropy than current implementations. Develop a test suite based on a standard test, (for example NIST Special Publication 800-22 or equivalent), to demonstrate an improved (higher level) of entropy provided by their FPGA PUF. We are interested in authentication PUF with much less than 1 part in 10 million chance of a false positive authentication. We are also interested in PUF based random number generators. Participation in this SBIR is limited to US citizens and US persons.

PHASE I: Research the feasibility of developing a FPGA based physical unclonable function with improved (higher) entropy than current implementations. Research the feasibility of creating PUF based random number generator(s), and PUF based authentication algorithm(s). Propose a verification test to estimate the lower bound for the entropy of the PUF. Propose a test to estimate a lower bound for the security level of the proposed PUF. Provide the government point of contact with a phase I final report.

PHASE II: Develop a field programmable gate array, intellectual property (IP) block implementing the physical unclonable function based on the phase I research. Develop a PUF based random number generator, and a PUF based authentication algorithm. An independent lab is to test and evaluate the performance of the PUF. Provide the government point of contact with a copy of the test and evaluation report. Provide the government point of contact a license for 2 PUF intellectual property blocks for testing and evaluation. At the government's facility, provide a 2 day on site seminar on the PUF. Provide the government point of contact a final report.

PHASE III-DUAL USE APPLICATIONS: Department of Defense Directive (DOD) 5000.2R provides instructions on identifying critical technologies and on defining methods to protect them. Commercialization opportunities exist throughout the Defense Department and within the government agencies such as the Department of Homeland Security and Intelligence Community for technologies to protect critical technologies. Applications for a

commercial version of the technology include protection of hardware and software intellectual property.

REFERENCES:
[1] C. O'Donnell, et al.: "PUF Based Random Number Generation," MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) Technical Memo 481, Nov. 2004, November. http://csg.csail.mit.edu/pubs/memos/Memo-481/Memo-481.pdf

[2] S. Kumar, et al.: "Extended abstract: The butterfly PUF protecting IP on every FPGA," IEEE International Workshop on Hardware-Oriented Security and Trust, pp. 67 - 70, June 2008.

[3] J. Guajardo, et al.: "Brand and IP protection with physical unclonable functions," IEEE International Symposium on Circuits and Systems, pp. 3186 - 3189, May 2008.

[4] P. Tuyls, et al.: "An information theoretic model for physical unclonable functions," IEEE Proceedings of the International Symposium on Information Theory, p. 141, June/July 2004.

[5] J. Guajardo, et al.: "Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection," IEEE International Conference on Field Programmable Logic and Applications, pp. 189 - 195, Aug. 2007.

[6] G. Suh and S. Devadas: "Physical Unclonable Functions for Device Authentication and Secret Key Generation," ACM/IEEE Design Automation Conference, pp. 9 - 14, June 2007.

[7] J. Huang and J. Lach: "IC activation and user authentication for security-sensitive systems," IEEE International Workshop on Hardware-Oriented Security and Trust, pp. 76-80, June 2008.

[8] D. Puntin, et al.: "CMOS unclonable system for secure authentication based on device variability," IEEE European Solid-State Circuits Conference, pp. 130 - 133, Sept. 2008.

[9] M. van Dijk, et al.: "Reliable Secret Sharing With Physical Random Functions," MIT Computer Science and Artificial Intelligence Laboratory, Computation Structures Group Memo 475, Dec. 2004. http://csg.csail.mit.edu/pubs/memos/Memo-475/Memo-475.pdf

[10] L. Bassham III: "The Random Number Generator Validation System (RNGVS)," NIST Computer Security Division, Jan. 2005. http://csrc.nist.gov/groups/STM/cavp/documents/rng/RNGVS.pdf

[11] A. Rukhin et al.: "A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications," NIST Special Publication 800-22 Rev 1 (dated August 2008), http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html

[12] NIST: "Security Requirements for Cryptographic Modules," FIPS 140-2, May 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

KEYWORDS: FPGA, field programmable gate array, provable unclonable function, physical unclonable function, PUF, reverse engineering, anti-tamper.

OSD10-A03 TITLE: System Configuration Verification

TECHNOLOGY AREAS: Information Systems, Materials/Processes

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), which controls the export and import of defense-related material and services. Offerors must disclose any proposed use of foreign nationals, their country of origin, and what tasks each would accomplish in the statement of work in accordance with section 3.5.b.(7) of the solicitation.

OBJECTIVE: Develop new innovative technology or techniques to verify that a system's configuration matches the intended baseline configuration as a normal part of its startup routine, in order to detect system modification or tampering. Configuration verification should reliably confirm that circuit boards, components, cables, and software/firmware are in the correct, trusted configuration before system operation. The technology or techniques should be low cost, low/zero power, small form factor, covert, and effective.

DESCRIPTION: The DoD has issued an instruction requiring the use of Anti-Tamper (AT) measures to protect Critical Program Information (CPI) from unintentional transfer. AT encompasses the systems engineering activities intended to prevent and/or delay exploitation of Critical Technologies (CT) in U.S. weapon systems. These activities involve the entire life-cycle of systems acquisition, including research, design, development, implementation, and testing of AT measures. Properly employed, AT will add longevity to a critical technology by deterring efforts to reverse-engineer, exploit, or develop countermeasures against a system or system component. AT is not intended to completely defeat such hostile attempts, but it should discourage exploitation or reverse-engineering or make such efforts so time-consuming, difficult, and expensive that even if successful, a critical technology will have been replaced by its next-generation version. Additional information on Anti-Tamper within the Department of Defense may be obtained at the DoD Anti-Tamper Executive Agent website, http://www.at.hpc.mil/index.htm.

The installation of monitoring, maintenance, debugging, and other analytical devices, as well as component or circuit board modification, represents a significant, long-standing threat to DoD critical technologies. The DoD is seeking new innovative technology or techniques to deter, prevent, detect, and respond to these threats to protect CPI, and preserve the warfighter's technological advantage. The focus of this topic is to verify the system configuration, and thereby detect any efforts by the adversary to tamper with, or modify the system. Such measures could be integrated with a combination of other measures to add an additional layer of protection, without significantly changing the appearance, functionality, or performance of the system. Though the particular solution may be tailored to an individual design, the concept and methodology of the solution should be applicable to various COTS and military hardware.

The techniques can be either hardware or software focused, but an integrated hardware/software solution is the ideal. The technique should be able to be configured to respond appropriately if system configuration can't be verified. The technique should be able to be integrated with other protection techniques for a robust protection solution. The technique should be able to detect configuration changes and configuration spoofing attempts. The desired technology or techniques could work in both US fielded systems and US systems sold through foreign military sales.

PHASE I: The contractor shall develop the conceptual framework for new and innovative System Configuration Verification technology or technique that is integrated with the system being protected. The contractor will also perform an analysis and limited bench level testing to initially assess the effectiveness, cost, size, power consumption, and other pertinent characteristics of the prototype solution.

PHASE II: Demonstrate and validate the use of the System Configuration Verification technology or technique into one or more prototype efforts and estimate the effectiveness and implementation considerations of the technology or technique. A partnership with a current or potential supplier of DoD systems, subsystems or components is highly desirable. Identify any commercial benefit or application opportunities of the innovation.

PHASE III DUAL-USE APPLICATIONS: Integrate the selected System Configuration Verification technology or technique into a DoD system or subsystem to proof the technology or technique. This phase will demonstrate the ability of the technology or technique to effectively protect against one or more reverse engineering threats, while meeting the programs need for cost, schedule, reliability, and system performance. This phase will result in a mission ready product that is available for immediate integration into a DoD system.

REFERENCES:

[1] Under Secretary of Defense for Intelligence. (2008). Critical Program Information (CPI) Protection Within the Department of Defense (DODI-5200.39). Retrieved July 7, 2009, from http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf

[2] Anti-Tamper / Software Protection Initiative. (2009). Introduction to Anti-Tamper. Retrieved July 7, 2009, from http://www.at.hpc.mil/index.htm

KEYWORDS: Anti-Tamper, Verification, Validation, Test Equipment, Reverse Engineering, Covert, Low Power

OSD10-A04 TITLE: Anti-Reverse Engineering (RE) Techniques

TECHNOLOGY AREAS: Information Systems, Materials/Processes

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), which controls the export and import of defense-related material and services. Offerors must disclose any proposed use of foreign nationals, their country of origin, and what tasks each would accomplish in the statement of work in accordance with section 3.5.b.(7) of the solicitation.

OBJECTIVE: Research and develop technology, tools, and/or fabrication/design guidelines and methods to prevent, identify, or severely limit reverse engineering (RE) techniques on microelectronic devices.

DESCRIPTION: The majority of critical technologies are contained within microelectronic devices, such as ASICs or FPGAs. Therefore, these devices will be targeted by an exploiter to extract or reveal protected information. Technology and methods are needed to detect and/or prevent reverse engineering techniques available to the adversary.

Reverse Engineering techniques to be considered include the following:
- Physical (Depackaging, Delayering, and Probing)
- Imaging (Optical, and SEM - Scanning Electron Microscope)
- Glitching (Power, Laser, Environmental, and Timing)
- Side channel (SPA - Simple Power Analysis, DPA - Differential Power Analysis, HO-DPA - High-Order Differential Power Analysis, and DFA - Differential Fault Analysis).

Participation in this SBIR is limited to US citizens and US persons.

PHASE I: Research the above RE techniques, and countermeasures for microelectronic devices. The contractor will then identify which anti-RE technology areas are going to be developed with approval from the government. The anti-RE technologies must not significantly degrade system performance. Simulations, simple prototypes, and/or models may be developed to demonstrate the feasibility of anti-RE technologies. Provide a final report to the government describing the proposed anti-RE technologies, and summarizing the findings of the RE techniques and countermeasures research.

PHASE II: Develop a prototype anti-RE technology(ies) based on phase I research. An independent lab is to test and evaluate the anti-RE technologies prototype, and provide a copy of the test and evaluation report to the government. Provide one (1) prototype anti-RE technology to the government point of contact for testing and evaluation. At the government's facility, provide a 2 day on site seminar covering the anti-RE technology. Provide a final report to the government point of contact.

PHASE III DUAL USE APPLICATION: Department of Defense Directive (DOD) 5000.2R provides instructions on identifying critical technologies and on defining methods to protect them. Commercialization opportunities exist throughout the Defense Department and within the government agencies such as the Department of Homeland Security and Intelligence Community for technologies to protect critical technologies. Applications for a commercial version of the technology include protecting hardware/software intellectual property.

REFERENCES:
[1] Wills, L., Newcomb, P., Eds. Reverse Engineering, Kluwer Academic Publishers, 1996.

[2] Ingle, K. A. Reverse Engineering, McGraw-Hill Professional, 1994.

[3] Huang, A. Hacking the Xbox: An Introduction to Reverse Engineering, No Starch, 2003.

[4] Fullam, S. Hardware Hacking Projects for Geeks, O'Reilly, 2003.

[5] Grand, J., Russell, R., Mitnick, K. Hardware Hacking: Have Fun While Voiding Your Warranty, Syngress, 2004.

[6] Anderson, R., Kuhn, M. Tamper Resistance – A Cautionary Note, Cambridge, 1996.

[7] Menezes, P., Oorschot, V., Vanstone, S. Handbook of Applied Cryptography, CRC, 1996.

[8] Nohl, K., Evans, D. Reverse Engineering a Cryptographic RFID Tag, University of Virginia, 2007.

[9] Torrance, R., James, D. Reverse Engineering in the Semiconductor Industry, Chipworks, 2007.

[10] Kocher, P., Jaffe, J., Jun, B. Intro to Differential Power Analysis and Related Attacks, CRI, 1998.

KEYWORDS: Anti-tamper, Reverse Engineer, Design, Fabrication, Techniques, and Methods.

OSD10-A05 TITLE: Tamper Resistant UAV/UGV Embedded Architecture

TECHNOLOGY AREAS: Information Systems, Materials/Processes

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), which controls the export and import of defense-related material and services. Offerors must disclose any proposed use of foreign nationals, their country of origin, and what tasks each would accomplish in the statement of work in accordance with section 3.5.b.(7) of the solicitation.

OBJECTIVE: Develop a tamper resistant, multiprocessor, embedded computer system architecture consisting of a microprocessor, a digital signal processor (DSP), a field programmable gate array (FPGA), and a graphics processing unit (GPU).

DESCRIPTION: Embedded computers are progressing towards multiprocessor solutions where each “processor” is optimized for a specific task. For example, a flight control computer might consist of the following commercial-off-the-shelf (COTS) integrated circuits: microprocessor, DSP, FPGA, and GPU (system dynamics and matrix intensive operations are performed by a graphics processing unit).

The proposed architecture may serve as a basic computer building block for computation intensive embedded computing systems. A goal of the proposed architecture is to create a reconfigurable computer system that can be optimized for different applications: UAV, UGV, or other embedded systems.

We are interested in anti-tamper techniques that can be applied across several levels for the multiprocessor architecture. Anti-tamper technologies protect system hardware, software, and firmware. We are not interested in tamper resistance designs where a volume protection or a coating is the fundamental protection layer. We are not interested in solutions that are primarily information assurance based. Embedded systems are typically power limited. Power saving and power management features will be consider a plus. Participation in this SBIR is limited to US citizens and US persons.

PHASE I: Research the feasibility of developing a tamper resistant, multiprocessor, embedded computer system architecture consisting of a microprocessor, DSP, FPGA, and GPU. To demonstrate the feasibility of the proposed tamper resistant multiprocessor architecture, models, simulations, and/or prototypes may be developed. Propose a model based design approach for developing hardware/reconfigurable logic/software for the “Tamper Resistant UAV/UGV Embedded Architecture.” Provide the government point of contact, a midterm and a final report describing the proposed tamper resistant embedded computer system architecture and proposed model based design methodology.

PHASE II: Develop a tamper resistant, prototype multiprocessor embedded computer architecture consisting of a microprocessor, DSP, FPGA, and GPU and incorporate hardware tamper protection. Develop and simulate an UAV navigation system using model based design. Target the components from the model based design/simulation towards "Tamper Resistant UAV/UGV Embedded Architecture," (embedded multiprocessor computer architecture.) Apply any operating system/application software/etc. level protections. An independent lab is to test and evaluate the tamper protection features of the prototype navigation system. Provide a copy of the independent lab evaluation report to the government point of contact. Deliver one (1) prototype embedded multiprocessor computer architecture, model based design software tools, and all required software develop tools to the government for testing and evaluation. Provide three days of onsite (at the government's facility) training for the "Tamper Resistant UAV/UGV Embedded Architecture." Provide a final phase II report.

PHASE III-DUAL USE APPLICATIONS: Department of Defense Directive (DOD) 5000.2R provides instructions on identifying critical technologies and on defining methods to protect them. Commercialization opportunities exist throughout the Defense Department and within the government agencies such as the Department of Homeland Security and Intelligence Community for technologies to protect critical technologies. Applications for commercial versions of the embedded multiprocessor architecture include: high performance computation intensive embedded computing, digital signal processing, and image processing.

REFERENCES:

[1] H. Christophersen, et al.: "Small Adaptive Flight Control Systems for UAVs using FPGA/DSP Technology," Georgia Institute of Technology, Atlanta GA, 2004. http://www.ae.gatech.edu/~ejohnson/uav2004_fcs20.pdf

[2] J. Owens, et al.: "GPU Computing," Proceedings of the IEEE, Vol. 96, Issue 5, pp. 879 – 899, May 2008.

[3] Z. Baker, et al.: "Matched Filter Computation on FPGA, Cell and GPU," IEEE Symposium on Field-Programmable Custom Computing Machines, pp. 207 – 218, April 2007.

[4] J. Brown: "High Performance Processor Development for Consumer Electronics Game Processor Perspective," IEEE Symposium on VLSI Circuits, pp. 112 – 115, June 2007.

[5] I. Buck: "GPU Computing: Programming a Massively Parallel Processor," IEEE International Symposium on Code Generation and Optimization, p. 17, March 2007.

[6] M. Macedonia: "Why Graphics Power Is Revolutionizing Physics," IEEE Computer, pp. 91 – 92, Vol. 39, Issue 8, Aug. 2006.

[7] R. McMurran, et al,: "Model based validation techniques for complex control systems," The Institution of Engineering and Technology Hybrid Vehicle Conference, pp. 201 - 212 , Dec. 2006.

[8] J. Langenwalter: "Embedded automotive system development process - steer-by-wire system," IEEE Proceedings of the Design, Automation and Test in Europe, Vol. 1, pp. 538 - 539, 2005.

KEYWORDS: Microprocessor, field programmable gate array, digital signal processor, graphics processor unit, FPGA, DSP, GPU, reverse engineering, tamper proof, anti-tamper, model based design, navigation, cell processor

OSD10-A06 TITLE: FPGA Bit Stream Data Electromagnetic Field Analysis

TECHNOLOGY AREAS: Materials/Processes, Sensors

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), which controls the export and import of defense-related material and services. Offerors must disclose any proposed use of foreign nationals, their country of origin, and what tasks each would accomplish in the statement of work in

accordance with section 3.5.b.(7) of the solicitation.

OBJECTIVE: Research the existence, detection and analysis of an electromagnetic field (EMF) radiated during FPGA bit stream operation.

DESCRIPTION: Most items found to be critical technologies in DoD weapon systems are related to underlying software. A common protection method for software-based technologies is encryption. Recent public literature papers (1)-(7) examine the potential of electromagnetic fields reducing the security level of a system. If such a field can be detected and interpreted, it would reduce the security. The proposed detector will analyze EMF flux density, field changes over time and other properties as needed to reveal the data content. Unlike physical attack, EMF analysis may be non-invasive, easily automated and not require knowing the design of the device under test. In most cases, an adversary will not attempt a direct attack on the encrypted information itself but will search for the encryption keys. The goal of such analysis would be the extraction of said keys. Participation in this SBIR is limited to US citizens and US persons.

PHASE I: Offerer will research the feasibility of developing an electromagnetic (electric field and/or magnetic field) detector(s) to analyze and interpret the electromagnetic fields radiated during a FPGA bit stream data operation. Offerer may develop simulations, simple prototypes, and/or models to research the feasibility of analyzing and interpreting electromagnetic fields radiated during a FPGA bit stream data operation. Offerer will submit a final report to the government describing the proposed technology.

PHASE II: Offerer will select a field programmable gate array for phase II. Offerer will develop a prototype system to analyze and interpret the electromagnetic fields radiated during a FPGA bit stream data operation based on the phase I research. With Government concurrence, the offerer will have an independent lab test and evaluate the proposed technology. Offerer will provide a copy of the test and evaluation report to the government. Offerer will provide one (1) prototype system and all required software tools to the government point of contact for testing and evaluation. Offerer will provide a final report describing the system to analyze and interpret the electromagnetic fields radiated during a FPGA bit stream data operation. At the government's facility, the offerer will provide a 2 day on site training for the prototype. A final report will be provided to the government.

PHASE III DUAL-USE APPLICATIONS: Department of Defense Directive (DOD) 5000.2R provides instructions on identifying critical technologies and on defining methods to protect them. Commercialization opportunities exist throughout the Defense Department and within the government agencies such as the Department of Homeland Security and Intelligence Community for technologies to protect critical technologies. Applications for a commercial version of the technology include protecting hardware and software IP.

REFERENCES:

[1] E. de Mulder, et al.: "Differential Electromagnetic Attack on an FPGA Implementation of Elliptic Curve Cryptosystems," IEEE World Automation Congress, pp. 1 – 6, July 2006.

[2] Y. Zafar and D. Har: "A Novel Countermeasure Enhancing Side Channel Immunity in FPGAs," IEEE International Conference on Advances in Electronics and Micro-electronics, pp. 132 – 137, Sept./Oct. 2008

[3] S. Braun, et al.: "A novel realtime time-domain EMI measurement system based on field programmable gate arrays," IEEE 17th International Zurich Symposium on Electromagnetic Compatibility, pp. 501 – 504, Feb./Mar. 2006.

[4] X. Dong, et al.: "Analysis of chip-level EMI using near-field magnetic scanning," IEEE International Symposium on Electromagnetic Compatibility, Vol. 1, pp. 174 – 177, Aug. 2004.

[5] R. Perez: "Signal integrity issues in ASIC and FPGA design," International Symposium on Electromagnetic Compatibility, pp. 334 – 339, Aug. 1997.

[6] C. Irvine, and K. Levitt: "Trusted Hardware: Can It Be Trustworthy?," IEEE Design Automation Conference, pp. 1 – 4, June 2007.

[7] P. Eskelinen, et al.: "Mobile security - in search for comprehensive integrity," Fifth IEE International Conference on 3G Mobile Communication Technologies, pp. 457 – 460, 2004.

KEYWORDS: Electromagnetic field, field programmable gate array, FPGA, Sensors, Electronics

OSD10-A07 TITLE: Incorporation of trust into integrated circuit (IC) and field programmable gate array (FPGA) design

TECHNOLOGY AREAS: Information Systems, Materials/Processes

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), which controls the export and import of defense-related material and services. Offerors must disclose any proposed use of foreign nationals, their country of origin, and what tasks each would accomplish in the statement of work in accordance with section 3.5.b.(7) of the solicitation.

OBJECTIVE: Develop innovative trusted intellectual property (IP) (circuit designs, embeddable micro-code, and the like) that will prevent other portions of an integrated circuit (IC) or field programmable gate array (FPGA) design from operating in modes, malicious or accidental, other than those intended by the designer.

DESCRIPTION: In the modern process of integrated circuit (IC) development, the actual design and fabrication of an IC typically is distributed between a number of different companies and/ or individuals. Often, a design house for a new IC will design some of their own intellectual property (IP) components while purchasing other IP components from other vendors. Typically, the source code for these purchased components is not available to the designer, who, instead, relies on interface control documents (ICDs) and programming interface descriptions. This requires a degree of trust between the designer and the IP vendor: the designer trusts that the vendor has listed all the functionality of the IP he is providing, and that no other functions from this IP core are possible.

Additionally, in the manufacturing of devices by independent IC foundries, the foundry will often take the designer's original design and include into it foundry-specific circuitry for testing, in order to assure yields at the wafer level. This would be another part of the design process over which the original designer has no control.

Ultimately, the original designer wants to be able to assure that the final device performs only those functions for which it was designed and no others. The goal of this task is to develop IP cores that can be incorporated into a design such that the functioning of non-trusted IP can be monitored and controlled. Participation in this SBIR is limited to US Citizens and US persons.

PHASE I: The offeror will investigate methods for unambiguously specifying the intended operation of a system. Additionally, the offeror will perform a preliminary design of IP cores or systems of IP specifically for the purpose of implementing the trusted operation as described in the first phase of this task, assuring trust in overall IC and FPGA designs. These cores will monitor the performance of other IP on the device, signaling and/or preventing anomalous, unintended operations. The performance of whatever approach is taken needs to be verified via simulation, at least to the transaction level or to whatever level is most appropriate for the proposed approach. The offeror will provide a final report to the government.

PHASE II: In the second phase, the contractor will more fully develop the approaches determined to be most promising in Phase I. The contractor will propose a system based on a mix of IP. The offerer will demonstrate that, even if a piece of IP on the system performs in a malicious way (i.e. it is malware), the integrity of the overall system is not compromised. Ideally, by the end of Phase II, the offerer should be able to demonstrate this in an FPGA environment. The offeror will provide a two day on site seminar covering the IP components and the system. The offeror will provide a final report to the government.

PHASE III: Dual Applications: Department of Defense Directive (DOD) 5000.2R provides instructions on identifying critical technologies and on defining methods to protect them. Commercialization opportunities exist throughout the Defense Department and within the government agencies such as the Department of Homeland

Security and Intelligence Community for technologies to protect critical technologies. Commercial applications include manufacturing companies who want to protect their IP during the design/fabrication of hardware and software.

REFERENCES:
[1] Adee, Sally, IEEE Spectrum, "The Hunt for the Kill Switch," http://www.spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0

[2] Pope, S., "Trusted Integrated Circuit Strategy," IEEE Transactions on Components and Packaging Technologies, vol. 31, iss. 1, March 2008, pgs. 230-234.

[3] Trimberger, S, "Trusted Design in FPGAs," Design Automation Conference, 2007, DAC '07, 44th ACM/IEEE, 04-08 June 2007, pgs. 5-8.

[4] Verbauwhede, I. , Schaumont, P, "Design Methods for Security and Trust," Design, Automation & Test in Europe Conference and Exhibition, 2007, DATE '07, 16-20 April 2007, pgs. 1-6.

KEYWORDS: IC, FPGA, Trusted Intellectual Property (IP), Trusted Design, Trusted Operation

OSD10-A08 TITLE: Intellectual Property (IP) in untrusted fabrication environments

TECHNOLOGY AREAS: Materials/Processes

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), which controls the export and import of defense-related material and services. Offerors must disclose any proposed use of foreign nationals, their country of origin, and what tasks each would accomplish in the statement of work in accordance with section 3.5.b.(7) of the solicitation.

OBJECTIVE: Develop methods and designs for allowing for the determination that no unintended functionality has been added to a hardware device in the time between when the design is provided to the foundry and when the finished device is provided to the user.

DESCRIPTION: In the modern process of integrated circuit (IC) development, the actual design and fabrication of an IC typically is distributed between a number of different companies and/ or individuals. This is the "modus operandi" of what are called "fabless" design houses: the designs are performed by this company, but the layout, mask fabrication, and actual IC fabrication are contracted out to other companies. Almost by necessity, this same approach is taken for application specific integrated circuit (ASIC) development: the "customer," the entity with the most in-depth knowledge of the required functionality of the device, will do the high-level design of the device, perhaps working at the schematic capture or hardware design language (HDL) level of the design. They may do some preliminary layout of the device, as well. The customer will also perform the required simulation and verification to assure that the device will perform as expected when it is actually fabricated. At this point, the design is typically handed off to an actual IC foundry for manufacture of the masks and then the manufacture of the ICs, themselves.

After the manufacture of the ICs by the foundry, samples of the chips are returned to the original customer for hardware verification. However, verification typically covers only the desired operations of the chip; that is, the chip is shown to perform those functions for which it was designed. It is not usually the case that the chip is shown to perform no other action than those for which it was designed. This situation requires a degree of trust between the design house and the foundry, the design house trusting that no additional undocumented functionality has been added to its original design. It is for this reason that the government has set up the "Trusted Foundry" program. However, going this route rather than taking advantage of competitive foundries can significantly impact the cost of a design program.

It is desired that methodologies be developed that allow the design house to verify not only that a device received

from the foundry provides those functions for which it was specifically designed, but that it performs no other functions. Participation in this SBIR is limited to US citizens and US persons.

PHASE I: In the first phase, the offerer will propose and verify hardware verification methodologies for insuring both positive (the device does what it is supposed to do) and negative (the device does nothing other than what it is supposed to do) compliance to a design specification. This compliance verification will occur at least at the transaction level. The offerer will provide a final report to the government.

PHASE II: Taking a design of reasonable complexity, the offerer will demonstrate that any added or deleted functionality is revealed in the final hardware validation. If applicable, this will be verified using an actual FPGA implementation. The offerer will show how this methodology will scale to larger applications and, more specifically, to ASIC designs. The offerer will provide a 2 day on site seminar covering the methodology. A final report will be provided to the government.

PHASE III-DUAL APPLICATIONS:
The offerer will continue to develop this verification methodology for incorporation into commercial hardware design suites. This can be through integrating the selected system configuration/verification of trusted fabrication applied to all integrated circuit commercial companies, especially in electronics.

REFERENCES:
[1] Adee, Sally, "The Hunt for the Kill Switch," IEEE Spectrum, http://www.spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0

[2] Pope, S., "Trusted Integrated Circuit Strategy," IEEE Transactions on Components and Packaging Technologies, vol. 31, iss. 1, March 2008, pgs. 230-234.

[3] Irvine, C.E., Levitt, K., "Trusted Hardware: Can It Be Trusted?" Design Automation Conference, 2007, DAC '07, 44th ACM/IEEE, 4-8 June 2007, pgs. 1-4

[4] Verbauwhede, I. , Schaumont, P, "Design Methods for Security and Trust," Design, Automation & Test in Europe Conference and Exhibition, 2007, DATE '07, 16-20 April 2007, pgs. 1-6.

[5] Khasidashvili, Z., et al, "Post-reboot Equivalence and Compositional Verification of Hardware," Formal Methods in Computer Aided Design, 2006, FMCAD '06, Nov. 2006, pgs. 11-18.

[6] Clarke, E., Kroening, D., "Hardware Verification using ANSI-C programs as a reference," Design Automation Conference, 2003, Proceedings of the ASP-DAC 2003, Asia and South Pacific, 21-24 January 2003, pgs 208-311.

[7] Biere, A., et al, "Symbolic model checking using SAT instead of BDDs," Design Automation Conference, 1999, Proceedings, 36th, 21-25 June 1999, pgs. 317-320.

KEYWORDS: Integrated Circuit, Manufacturing, Fabrication, IP, Verification, Hardware Design, MDL, ASIC

OSD10-A09 TITLE: Zero Power/Ultra Low Power Tamper Detection Sensors

TECHNOLOGY AREAS: Materials/Processes, Sensors

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), which controls the export and import of defense-related material and services. Offerors must disclose any proposed use of foreign nationals, their country of origin, and what tasks each would accomplish in the statement of work in accordance with section 3.5.b.(7) of the solicitation.

OBJECTIVE: Develop zero power/ultra low power tampering/reverse engineering sensor technology for use at the printed circuit board level, or integrated circuit level.

DESCRIPTION: Recent developments in nanotechnology sensors, and micro-electromechanical systems (MEMS) offer opportunities for creating ultra low power sensors to detect tampering and reverse engineering. The purpose of this SBIR is to develop tampering/reverse engineering sensors for the printed circuit board, or integrated circuit level that require zero power or near zero power (in the 0.1 to 1 microwatt range).

Energy harvesting technologies may also be beneficial for ultra low power sensor technologies. We are not interested in materials that require visual inspection for tamper detection. We are not interested in material coatings for printed circuit boards or integrated circuits.

Participation in this SBIR is limited to US citizens and US persons.

PHASE I: Research the feasibility of developing zero power/ultra low power sensors (< 1 microwatt continuous power consumption) for tamper detection and reverse engineering detection. We are not interested in low duty cycle sensors to reduce power consumption (e.g. 1 % duty cycle at 0.1 milliwatts gives 1 microwatt average power consumption). To demonstrate the feasibility of zero power/ultra low power sensors, simulations, simple prototypes, and/or models may be developed. Estimate the power consumption of the proposed sensor technology and estimate its sensitivity to detecting a tamper event. Provide a phase I final report to the government point of contact.

PHASE II: Based on the phase I research, develop a prototype zero power or ultra low power tamper sensor. For ultra low power tamper sensor development, research and develop methods to further decrease power consumption. An independent lab is to test and evaluate the zero power/ultra low power tamper sensor technology. A copy of the test report is to be provided to the government point of contact. This test and evaluation is a potential opportunity for future commercialization. Deliver to the government point of contact, two tamper sensor evaluation boards, and all required software tools for testing and evaluation. Provide an on-site two day sensor system seminar at a government's facility. Provide a phase II final report to the government point of contact.

PHASE III-DUAL USE APPLICATIONS: Department of Defense Directive (DOD) 5000.2R provides instructions on identifying critical technologies and on defining methods to protect them. Commercialization opportunities exist throughout the Defense Department and within the government agencies such as the Department of Homeland Security and Intelligence Community for technologies to protect critical technologies.
A commercial version of the technology could be used to protect hardware/software intellectual property (IP).

REFERENCES:
[1] K. Greene: "Memristors Make Chips Cheaper: The first hybrid memristor-transistor chip could be cheaper and more energy efficient," 25 Nov. 2008. http://www.technologyreview.com/alt-thinking/hp_feature_article.aspx?id=21710&pg=1

[2] M. Hirose: "Challenge for future semiconductor development," IEEE International Microprocesses and Nanotechnology, pp. 2-3, Nov. 2002.

[3] C. Fung and W. Li: "Ultra-low-power polymer thin film encapsulated carbon nanotube thermal sensors," IEEE Conference on Nanotechnology, pp. 158 - 160, Aug. 2004.

[4] S. Shanbhag: "CMOS integrated circuit for sensing applications," IEEE VLSI Design, p. 4, Jan. 2006.

[5] K. Najafi: "Low-power micromachined microsystems," ACM Proceedings of the 2000 International Symposium on Low Power Electronics and Design, p. 1-8, 2000.

[6] Y. Yao, et al.: "Surface Plasmon Resonance Biosensors and its Application," The 1st International Conference on Bioinformatics and Biomedical Engineering, pp. 1043 - 1046, July 2007.

[7] K. Bourzac: "TR10: Nanopiezoelectronics," Technology Review, MIT, March/April 2009. http://www.technologyreview.com/energy/22118/

[8] R. Adam, et al.: "Current induced switching of magnetic tunnel junctions," IEEE International Magnetics Conference, p. GD - 06, March/April 2003.

[9] C. Lo and Y. Huang: "High performance bipolar spin transistor," IEEE International Conference on Solid-State and Integrated Circuits Technology, Vol. 1, pp. 746 - 751, Oct. 2004.

KEYWORDS: microelectromechanical systems, MEMS, nanotechnology, magnetic, sensor, ultra low power, integrated circuit, piezoelectric, nanomaterials, thin film, plasmon, memristor, photonics, tamper resistant, reverse engineering, anti-tamper

OSD10-CR1 TITLE: Rapid Assessment of Team Cognitive Readiness

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: The objective of this topic is to develop a sensor and analysis suite that rapidly assesses the cognitive readiness of teams before – or as they are – participating in military operations.

DESCRIPTION: Current and future combat operations will continue to place a strong emphasis on team and joint operations. As with individual Warfighters, it is vitally important for commanders and leaders to have the ability to quickly assess the overall cognitive readiness of these teams and joint groups, before and during military operations. Team cognitive readiness represents a unique extension of individual cognitive readiness in that it is an outcome of individuals joining together for the purpose of exploiting one another's individual skills to successfully accomplish a common goal [1]. On the other hand, while much is known about how individuals develop skills [2,3,4], comparatively less is known about how team skills develop and how team members work together as a coordinated unit. Importantly, team cognitive readiness is not simply a linear combination of individual members' cognitive readiness, because often times different individual levels of readiness may combine constructively or destructively. Consequently, it is difficult to determine, using available assessment techniques, when a given team is at an effective level of cognitive readiness.

Current readiness metrics are based on team performance measures, which often use observational analysis coupled with expert evaluation [5,6], or event based measurements [7]. These measures ignore the temporal nature of team behavior and reveal little about the dynamic processes through which teams respond, evolve and develop [8]. Consequently they do not provide a solid enough foundation upon which to generate rapid assessments of cognitive readiness. Recent work that cuts across different domains – cognitive neuroscience, network science, non linear dynamics and neural-imaging sciences – has suggested that advanced measurement technologies and analytic techniques may be used to reveal the underlying basis for team coordination [9,10]. When these emerging approaches are combined with past work exploring the differences between effective and ineffective teams [11] a unique opportunity is presented to establish criteria and technologies for quickly assessing the cognitive readiness of teams.

The focus of this topic is on developing neurocognitive measures of team readiness, which can be detected and analyzed by a suite of sensors combined with analysis tools. This sensor suite, along with the to-be-developed metrics, should be capable of gathering individual and team level data (e.g. neural, cognitive and behavioral) as well as assessment-environment generated data, as required, to allow for the identification of the etiology and assessment of team cognitive readiness. The system should be able to complete data collection and assessment within a reasonable time frame, and with a small enough technical footprint, that it would not be disruptive of combat operations.

PHASE I: Define requirements for developing a technology that rapidly assesses the cognitive readiness of teams before they participate in military operations. Requirements definition must include: a description of the overall architecture that will be used to assess team cognitive readiness; a determination of the types and characteristics of metrics that will be captured and used; a detailed discussion of the analysis and assessment techniques to be used; and, a discussion of system performance metrics including both measures of effectiveness and measures of performance. Phase II plans should also be provided, to include key component technological milestones and plans

for testing and validation of the proposed system and its components. Phase I should also include the processing and submission of any necessary human subjects use protocols.

PHASE II: Develop a prototype system based on the preliminary design from Phase I. All appropriate engineering testing will be performed, and a critical design review will be performed to finalize the design. Phase II deliverables will include: (1.) a working prototype of the system, (2) specification for its development, (3) demonstration and validation of ability to rapidly assess team cognitive readiness and, (4) test data that demonstrates improved outcomes as a result of knowing the level of team cognitive readiness.

PHASE III: This technology will have broad application in military as well as commercial settings. Within the military, there is increasing emphasis on the ability of teams to operate in a distributed manner, away from direct observation from military commanders. Consequently tools that afford leadership the ability to monitor and assess these distributed teams' readiness are crucial to ensuring successful military operations. Similarly, in the commercial sector, teams –distributed or collocated –continue to play an important role in critical and high stress/high operations tempo environments like: Disaster relief, first responders, Air Traffic Control, Aviation. The proposed system should allow managers and team leads to gauge the current and projected readiness of their teams, enabling them to make critical personnel and manning decisions in near real time.

REFERENCES:

[1] Dyer, J. C. (1984). Team research and team training: A state of the art review. In F. A. Muckler (Ed.), Human factors review (pp.285-323). Santa Monica, CA: Human Factors Society.

[2] Fitts, P.M. (1964). Perceptual motor skills learning. In A.W. Melton (Ed.), Categories of human learning. (pp. 243-285). New York Academic Press.

[3] Dreyfus, H.C. & Dreyfus, S.E. (1980). A five-stage model of the mental activities involved in directed skill acquisition. ORC 80-2 (F49620-79-C-0063). Bolling, AFB, Washington, DC. Air Force Office of Scientific Research: United States Air Force.

[4] Ericsson, K.A., Krampe, R. Th., and Tesch-Romer, C., (1993). The role of deliberate practice in the acquisition of expert performance. Psychological Review, 700, p. 379 and p. 384.

[5] Brannick, M.T., Roach, R.M., & Salas, E. (1993). Understanding team performance: A multimethod study. Human Performance, 6:287-308.

[6] Modrick, J.A. (1986). Team performance and training. In J. Zeidner (Ed.), Human productivity enhancement: Training and human factors in systems design (Vol 1) New York: Praeger

[7] Fowlkes, J.E., Lane, N.E., Salas, E., Franz, T., & Oser, R. (!994). Improving the measurement of team performance: The TARGETs methodology. Military Psychology, 6:47-61.

[8] Buller, P.F.(1986) The team building-task performance relation: Some conceptual and methodological refinements. Group & Organizational Studies, 11:147-168.

[9] Oullier, O., DeGuzman, G.C., Jantzen, K.J., Lagarde, J., & Kelso, J.A.S. (2008). Social coordination dynamics: Measuring human bonding. Social Neuroscience, 3:178-192.

[10] Gorman, J. C., Hessler, E. E., Cooke, N. J., & Amazeen, P. G. (2009). Dynamics of team coordination and adaptive performance. 15th International Conference on Perception and Action, Minneapolis, MN.

[11] Glaser, R. (1996). Changing the agency for learning: Acquiring expert performance. In K. A. Ericsson (Ed.), The road to excellence (pp. 303-311). Mahwah, NJ: Lawrence Lawrence Erlbaum & Associates & Associates.

KEYWORDS: Cognitive Readiness, Team Performance, Assessment, Non linear, Neuroscience

OSD10-CR2 TITLE: Neuro Cognitive Control of Human Machine Systems

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: The objective of this topic is to develop a new approach to Human Machine Interfaces that uses neurocognitive markers of an operator's intended action to directly guide machine performance.

DESCRIPTION: The evolution of technology has created the potential to develop machines and systems that may exponentially increase the performance range of today's warfighter [1]. All too often, though, this improved performance comes with a high cost – increased sophistication and complexity of those very systems meant to improve performance [2]. As a result, the benefits of improved performance in one domain are offset by the cognitive costs of increased operator workload, decreased cognitive flexibility and delayed, incorrect, action [3]. Given the complex environments in which warfighters must operate on a daily basis, it is imperative that new human machine interaction (HMI) solutions be developed that enable warfighters to effectively use their machines without sacrificing cognitive readiness.

Control solutions that attempt to bridge this human- machine systems gap have typically emphasized engineering-centric solutions over human-centric ones and have met with limited success. The two most common engineering-centric solutions are automation technologies and brain computer interfaces. In a broad sense, automation is a means of substituting some machine actions for some human actions [4,5]. Today's automation solutions suffer from an inability to effectively perform these substitutions in novel, dynamic and mission-critical situations, maintaining a divide between humans and machines that can significantly increase time-to-act and introduce additional cognitive workload constraints [6,7,8]. Brain computer interfaces (BCI) use stereotypic and non specific neural signals to trigger predefined system outputs [9]. Because these neural signals are not directly correlated to the intended action, they require extensive training of the user to learn how to 'map' them onto desired system outputs – in effect, establishing a biofeedback loop, which could take weeks or even months [9]. Consequently, BCI systems do not easily scale with task complexity and cannot adapt to changing task environments and contexts. In short, today's human-machine systems control solutions play to the weaknesses of humans and the machines they operate – humans are quick to arrive at initial decisions but slow to develop plans to implement them, whereas machines have only limited ability to make effective decisions, but once provided with a desired outcome are quick to develop (and validate) plans to achieve it. An ideal control solution would support the strengths of both humans and machines, allowing them to work collaboratively within a shared action space.

The focus of this topic is on developing technologies that capture and use neurocognitive signals representing a human's intended action within a given task environment, providing this information to a machine to allow it to determine the optimal approach for achieving that intended action. This will revolutionize HMI by developing a neurocognitive control systems approach that plays to the strengths of humans, who are effective pattern detectors, and machines, which can quickly calculate and compare alternative courses of action. Anticipated benefits from using this neurocognitive control system include: orders of magnitude reduction in time-to-act; significant reduction in operator workload for using a single device; and significant increase in the number of devices a single human can control simultaneously.

PHASE I: Define requirements for developing a neurocognitive control system that will enable humans to operate machines more effectively. Requirements definition must include: at least one use case/application; a description of the architecture that will be used to capture operator intent, and translating these into a device control scheme; a determination of the types and characteristics of neurocognitive signals that will be captured and used; a detailed discussion of the overall system design that will enable neurocognitive – based interactions between humans and machines; and, a discussion of system performance metrics including both measures of effectiveness and measures of performance. Phase II plans should also be provided, to include key component technological milestones and plans for testing and validation of the proposed system and its components. Phase I should also include the processing and submission of any necessary human subjects use protocols.

PHASE II: Develop a prototype system based on the preliminary design from Phase I. All appropriate engineering testing will be performed, and a critical design review will be performed to finalize the design. Phase II deliverables will include: (1.) a working prototype of the system, (2) specification for its development, (3) demonstration and

validation of ability to record neurocognitive signals of intent and, (4) test data demonstrating capability to use these signals in a cognitive control system to guide machine action, assessed using measures of effectiveness and performance collected in one or more operational settings.

PHASE III: This technology will have broad application in military as well as commercial settings. With the increasing use of technically complex systems, military operators will find themselves experiencing significant cognitive overload. The proposed system will help reduce this stress. Similarly, as technology continues to become embedded in everyday work environments like disaster management, air traffic control, aviation, and other domains in which the human operator serves in a supervisory capacity the cognitive strain on users will increase. The proposed system should help to significantly reduce this stress. Another commercial application is within the medical rehabilitation industry, where the proposed system would help paralyzed and semi-paralyzed patients more effectively control devices (e.g. wheelchairs, prostheses etc) using neural signals only. Lastly, the commercial entertainment industry has long sought control interfaces that are neurally driven. The proposed system would provide a ready solution to this need.

REFERENCES:
[1] Scerbo, M.W. (1996). Theoretical perspectives on adaptive automation. In R. Parasuraman & M. Mouloua. (Eds.), Automation and human performance: Theory and applications (pp. 37-63). Mahwah, NJ: Lawrence Erlbaum Associates.

[2] Woods, D. D. (1996). Decomposing automation: Apparent simplicity, real complexity. In R. Parasuraman & M. Mouloua (Eds.), Automation and human performance: Theory and applications (pp. 3-18). Mahwah, NJ: Lawrence Erlbaum Assoc.

[3] Billings, C.E. (1997). Automation aviation. Mahwah, NJ: Lawrence Erlbaum Associates.

[4] Parsons, H. M. (1985). Automation and the individual: Comprehensive and comparative views. Human Factors, 27, 99-112.

[5] Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. Human Factors, 39, 230-253.

[6] Kirlik, A. (1993). Modeling Strategic Behavior in Human-Automation Interaction - Why an Aid Can (and Should) Go Unused. Human Factors 35(2), 221–42.

[7] Kreifeldt, J.G. & McCarthey, M.E. (1981). Interruption as a Test of the User-Computer Interface, in Proceedings of the 17th Annual Conference on Manual Control, JPL Pub. 81-95, pp. 655-67.

[8] McFarlane, D. (1997). Interruption of People in Human– Computer Interaction: A General Unifying Definition of Human Interruption and Taxonomy, Technical Report NRL/FR/5510-97-9870, US Naval Research Lab, Washington, DC.

[9] Dornhege, G., Millan, J.R., Hinterberger, T., McFarland, D.J., & Muller, K-R. (2007) Toward Brain Computer Interfacing, MIT Press, Cambridge MA.

KEYWORDS: Intent, Automation, Control Systems, Human Machine Interface, Cognitive

OSD10-CR3 TITLE: Immersive Scenario Based Training Environments for Intuitive Decision Making

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: The objective of this topic is to develop a capability to enhance and augment warfighters' intuitive decision making skills by embedding neurocognitive measures of intuition into immersive scenario based training applications.

DESCRIPTION: The shifting emphasis of warfare from symmetric and predictable to asymmetric and unpredictable, combined with changing military doctrine that provides greater autonomy to Warfighters, has placed an increasingly important requirement to develop Warfighters who are as cognitively ready as they are physically prepared [1]. One important consequence of this shifting emphasis is that our Warfighters are now being called upon to make decisions under vastly different operational situations and conditions. Whereas previous types of military missions may have allowed for logically reasoned responses to threats based on analyses of multiple sets of information, military missions in this new combat environment require a more dynamic kind of decision making, made under time constraints and based on partial or incomplete information [2,3,4]. This type of decision making is commonly referred to as 'intuitive decision making' or, more simply, as 'intuition' - a rapid, non-conscious, cue to the existence of meaningful information detected through one or more sensory modalities, often accompanied by affective and somatic reactions [5,6]. Intuition can be understood as the interaction between one's existing knowledge structures and incoming information enabling one to rapidly make sense of partial or incomplete information, and subsequently take necessary actions although they may not be fully understood [7,8]. Intuition therefore requires a level of domain knowledge in order to establish the required knowledge structures to make sense of incoming information [3].

The tight coupling between effective intuitive decision making and extensive domain knowledge suggests that the processes driving intuition may be improved through training. Moreover, because the type of knowledge that underlies effective intuitive decision making emphasizes an understanding of context, environment, and how relevant cues within those contexts and environments are perceived, the type of training most likely to support effective intuitive decision making should be experiential and interactive, instead of simply didactic and classroom based. Immersive environments, like virtual environments or serious games, present one approach for providing the kind of experiential and interactive experiences needed for training intuition [9,10]. Yet, immersive environments must still be populated with a training methodology. Scenario Based Training (SBT), which emphasizes embedding training approaches within an evolving and dynamic scenario, provides a promising technique for training in environments which require complex interactions supported by immersive technologies, such as virtual environments and serious games [11].

The focus of this topic is on leveraging recent advances in quantifying the neurcognitive dynamics of intuition [2, 12] and coupling these with Scenario Based Training approaches, within an immersive environment to enhance effective intuitive decision making. The final product would include an interactive environment, incorporating, neurcognitive tools to provide metrics that the system could then use to demonstrate trainee progression towards improving their intuitive decision making processes. Final product must include a system driven by SBT; actual system must be immerssive. For topic purposes, 'immerssive' spans a relatively broad category of systems from full sensory-immerssive systems providing full depth visual, haptic and audio stimulation to more cognitively and affectively immerssive systems in which the user experiences strong levels of Presence, as occurs with serious games. Regardless of technology level, system must demonstrate a means of integrating neurocognitive measures of intuition.

PHASE I: Define requirements for developing an immersive Scenario Based Training system for training intuitive decision making that is driven by neurocognitive and other types of performance measures. Identification of at least one military-relevant scenario, together with metrics definition is necessary. A final report will be generated, including system performance metrics and plans for Phase II. Metrics shall include both measures of effectiveness and measures of performance. Phase II plans should include key component technological milestones and plans for at least one operational test and evaluation. Phase I should also include the processing and submission of any necessary human subjects use protocols.

PHASE II: Develop a prototype system based on the preliminary design from Phase I. All appropriate engineering testing will be performed, and a critical design review will be performed to finalize the design. Phase II deliverables will include: (1.) a working prototype of the system, (2) specification for its development, and (3) test data on its performance collected in one or more operational settings using validated measures.

PHASE III: This technology will have broad application in military as well as commercial settings. The military requires its warfighters to make increasingly complex and important decisions under conditions of uncertainty and stress. The proposed system will provide today's warfighters with the ability to quickly hone their innate intuitive

decision making skills for a broad range of contexts and tasks. In a similar way, commercial workforce personnel in disaster management, air traffic control, and emergency medicine/first responders, and other environments in which decisions must be made under conditions of uncertainty and stress, will benefit from this type of training.

REFERENCES:
[1] DoD Directive 3000.07 (December 1, 2008).

[2] Luu, P., Geyer, A., Wheeler, T., Campbell, G., Tucker, D., & Cohn, J. (2010). The Neural Dynamics and Temporal Course of Intuitive Decisions. (Submitted) Public Library Of Science.

[3] Volz, K. G., & von Cramon, D. Y. (2006). What neuroscience can tell about intuitive processes in the context of perceptual discovery. Journal of Cognitive Neuroscience, 18(12), 2077-2087.

[4] Soldier's intuition and situational awareness a lifesaver in Iraq.(UPDATE ON Operation Iraqi Freedom) Publication: Army Reserve Magazine Publication Date: 22-MAR-07Author: Coleman, Chris COPYRIGHT 2007 U.S. Army Reserve.

[5] Hogarth, R.M (2001). Educating Intuition. University Of Chicago Press: Chicago, IL.

[6] Winerman, L. (2005). A 'sixth sense?' Or merely mindful caution? Monitor on Psychology, 36(3):62.

[7] Hodgkinson, G. P., Langan-Fox, J., & Sadler-Smith, E. (2008). Intuition: A fundamental bridging construct in the behavioral sciences. British Journal of Psychology, 99, 1-27.

[8] Bowers, K.S., Regehr, G., Balthazard, C.G., & parker, K. (1990). Intuition in the context of discovery. Cognitive Psychology, 22, 72-110.

[9]Lathan, C., Tracey, M., Sebrechts, M., Clawson, D., & Higgins, G. (2002). Using Virtual Environments as Training Simulators: Measuring Transfer In: Handbook of Virtual Environments: Design, Implementation, and Applications (Ed: Kay M. Stanney); Lawrence Erlbaum Associates, 2002 p. 403-414.

[10] Greitzer, F., Kuchar, O., Huston, K. (2007). Cognitive science implications for enhancing training effectiveness in a serious gaming context. Journal on Educational Resources in Computing 7(3).

[11] Oser, R.L., Cannon-Bowers, J.A., Salas, E. & Dwyer, D. J. (1999). Enhancing human performance in technology-rich environments: Guidelines for scenario based training. In E. Salas (Ed.), Human Technology Interaction in Complex Systems. JAI Press, Vol. 9 p. 175-202.

[12] Volz, K. G., Rubsamen, R., & von Cramon, D. Y. (2008). Cortical regions activated by the subjective sense of perceptual coherence of environmental sounds: a proposal for a neuroscience of intuition. Cognitive, Affective & Behavioral Neuroscience, 8(3): 318-328.

KEYWORDS: Intuition, Scenario Based Training, Neurocognitive, Decision Making, Virtual Environment

OSD10-CR4 TITLE: Training Battery for the Rapid Formation of Cognitively Ready, Effective Teams

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: The objective of this topic is to develop training and mitigation strategies to aid in the rapid formation of cognitively ready, highly effective and cohesive teams.

DESCRIPTION: In recent years organizational and military structure has moved from individual tasks to increasingly more collaborative efforts. Collaborative work has proved effective as each team member brings a different perspective, skill set, and knowledge set to the team which enables a more diversified, eclectic approach to

the project or mission. Ideally the formation of a team reduces workload and expedites effective mission completion however; the team approach introduces an additional layer of cognitive demands associated with the requirement to work effectively with others. Research shows that for a team to be effective they must possess a collection of task- and team-related knowledge held by teammates and their collective understanding of the current situation [1]. This requires that team members communicate clearly, share information freely and trust that each of their fellow team members will complete their tasks correctly and in a timely manner. In order to meet the mission requirements and time constraints of military operations the rapid development of highly effective teams is paramount [2]. This presents a challenge for team leaders as they must be able to quickly assess the knowledge, skills, abilities, and cognitive readiness of each team member and make key personnel decisions based on this assessment [3,4]. The relationship between cognitive readiness and team cohesion suggests that a training battery that assists in the augmenting of cognitive readiness during team formation could improve team cohesion and effectiveness.

The focus of this topic is to leverage current cognitive readiness, team cohesion, and team effectiveness research, metrics and measurements and couple them with current military team training strategies to develop a computerized training package that will enhance the cognitive readiness and effectiveness of a team [5]. The final product would include a battery of cognitive readiness assessment tools and team effectiveness tools that will enable team leaders to quickly assess the cognitive readiness of team members and based on those results suggest the appropriate mitigation and/or augmentation strategies to enable the team to perform at its full potential. The software must be compatible with all current Government and military computer systems.

PHASE I: The objective of Phase I is to develop the concept for the training battery. The contractor must define requirements for developing a training battery that is driven by cognitive and other types of performance measures. Identification of at least one military-relevant scenario, together with metrics definition is necessary. A final report will be generated, including system performance metrics and plans for Phase II. Metrics shall include both measures of effectiveness and measures of performance. Phase II plans should include developmental and technological milestones and plans for at least one test and evaluation event. Phase I should also include the processing and submission of any necessary human subjects use protocols.

PHASE II: The objective of Phase II is to develop a prototype training package based on the preliminary design from Phase I. All appropriate validation studies will be performed and a critical design review held to finalize the design of the training package. Phase II deliverables will include: (1) a working prototype of the training package software, (2) specification for its development, and (3) study data on its performance collected in one or more operational settings using validated measures.

PHASE III: This training could be marketed in a variety of military and civilian contexts in which individuals must routinely engage in effective, knowledgeable rapid team formation in an effort to achieve organizational goals. This training could serve as a complement to current leader knowledge and skill training taught at U.S. Army Command and General Staff College and other military education institutions.

REFERENCES:

[1] Cooke, Salas, Cannon-Bowers, Stout, (2002). "Measuring Team Knowledge." Human Factors, Volume 42.

[2] Urban, J., Bowers, C., Monday, S., and Morgan, B., (1995) "Workload, Team Structure, and Communication in Team Performance." Military Psychology. Volume 7.

[3] Cosenzo, KA, Fatkin, LT, Patton, DJ. Ready or not: enhancing operational effectivenss through use of readiness measures. Aviat Space Environ Med 2007; 78(5, Suppl.): B96-106.

[4] Cueves HM, Fiore SM, Caldwekk BS, Strater L. Augmenting team cognition in human-automation teams performing in complex operational environments. Aviat Space Environ Med 2007; 78(5, Suppl.): B63-70.

[5] Salas, E., Dickinson, T. L., Converse, S. A., and Tannenbaum, S. I. (992). Toward an understanding of team performance and training. In R. W. Swezey & E. Salas (Eds.), Teams: Their training and performance (pp. 3-29). Norwood, NJ: Ablex.

KEYWORDS: Team effectiveness; Team cohesion; Assessment

OSD10-CR5 TITLE: Generation of the Army Cognitive Readiness Assessment (ACRA)

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: Develop a new generation of the ACRA which would include additional functionality, faster data reduction, and great portability.

DESCRIPTION: In response to the Army's organizational goal of determining if the warfighter is mentally ready to carry out the mission, the Army funded a Small Business Innovative Research (SBIR) effort to construct a 'next generation' performance test battery designed to capitalize on past test battery developments and can be implemented in the field for operational assessment. As a result, a "next generation" cognitive performance testing system was developed that was more directly applicable to specific operational jobs than has been achieved in the past. For the first time, the capability existed to configure a test battery that was optimized for the specific job/task or class of job/tasks of interest. The tool is referred to as the Army Cognitive Readiness Assessment (ACRA) battery [1,2].

The ACRA identifies the cognitive markers predictive of combat readiness and uses the automated assessment of cognitive skills for enhancing the quality of human-systems integration. For instance, scores from the cognitive testing may be incorporated into technology evaluation models to assess the impact of a given system on overall mission performance. Moreover, by identifying under what circumstances task performance may be degraded can result in different requirements for the number or types of personnel needed for an operation in order to increase survivability [1,2].

The ACRA has proven to be a valuable tool to assess cognitive readiness however, the data extraction and reduction process is quite cumbersome and time consuming. This SBIR would further enhance the prototype ACRA system developed under the previous SBIR by incorporating it into an enhanced hardware/software configuration that would incorporate at least the following capabilities: 1) the entire T-Matrix test battery generation system already developed, with the added capability to modify the tests or matrix easily as additional data are generated, 2) a capability to accept a variety of physiological inputs including, as a minimum, eye and tremor behavior, 3) an enhanced analysis capability that would provide automated analysis and simplified data presentation phrased in the form of recommendations concerning the actual cognitive fightability of the soldier for the specific job or mission in question, and 4) a transmission capability that would allow these data and recommendations to be delivered to an operations center or headquarters.

PHASE I: Prepare a feasibility study for developing a next generation ACRA system that will provide more faster more efficient data reduction and reporting features that can be put in a hand-portable device. During the first phase the performer will propose a conceptual device and a preliminary design/architecture, to include descriptions of: technologies and the information presentation approach. A final report will be generated, including system performance metrics and plans for Phase II. Phase II plans should include key component technological milestones and plans for at least one operational test and evaluation using an operational system. Phase I should also include the processing and submission of all required human subjects use protocols.

PHASE II: Develop prototype system based on the preliminary design from Phase I. All appropriate testing will be performed, and a critical review will be performed to finalize the design. Phase II deliverables will include: (1) a working prototype of the technology (2) specification for its development, and (3) test data on its performance collected in one or more operational settings.

PHASE III: The ACRA is a computer based test battery and therefore is not ideal for studies conducted in more operationally realistic environments. A redesign of this tool that would enable greater portability, such as a personal digital assistant (PDA), would be a huge asset to conducting research studies in more operationally relevant environments as well as the test and evaluation of military systems.

REFERENCES:
[1] O'Donnell, R. D., Moise, S., & Schmidt, R. M. (2005). Generating performance test batteries relevant to specific operational tasks. Aviation, Space, and Environmental Medicine, 76(7), II Supplement.

[2] Swann, M., & Schmidt, R. M. (2005). Army cognitive readiness assessment: A next generation performance battery. Mira Digital Publishing: Human-Computer Interaction International Proceedings. CD-ROM.

KEYWORDS: Team readiness; assessment; cognitive performance

OSD10-CR6 TITLE: Distributed Team Workload Assessment Tool

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: The objective of this topic is to develop a scale capable of assessing the workload of a distributed, networked team.

DESCRIPTION: As technology continues to rapidly increase so does the level of complexity of many tasks found in modern work environments. This increase in complexity often leads to an exponential increase in workload. Working in teams is often viewed as an effective solution to completing complex tasks however; working in teams also present many challenges. The team approach adds an additional layer of cognitive requirements associated with the demands of working effectively with others [1]. For a team to be effective it is important that they possess team knowledge which can be defined as the collection of task- and team-related knowledge held by teammates and their collective understanding of the current situation [1]. In military situations teams are often rapidly formed by members that may not have any prior knowledge of fellow team members. In these situations workload can be influenced by many variables such as; trust, personality, work-style, skill-sets, etc. To compound these issues in many cases teams are distributed and networked. With the emphasis on joint-service operations, the formations of distributed teams have become a common occurrence. Within a networked environment team knowledge is vital as important decisions and key tasks must be completed by personnel whose workstations are in different locations. Each team member's individual task or decision point is usually directly influenced and/or dependent on those completed by their fellow team members. If an operator is overloaded they may miss out on important information that can help them in their decision making.

Extensive research has been conducted to identify the dimensions of teamwork, to assess individual workload, and to define and measure shared team knowledge [1-8] however, to date, the concept of distributed networked team workload has not been fully determined and explored.
This topic endeavors to leverage prior research on individual workload, expand it to include the concept of team workload and build upon it to include network parameters. The final product would include a tool, either a scale or model that can accurately assess the workload of a distributed and networked team as they strive to complete a mission.

PHASE I: Define requirements for developing a Distributed Team Workload Tool. Requirements definition must include: a description of the overall architecture that will be used to assess the workload of a distributed team; a description of the types and characteristics of metrics that will be captured and used; a detailed discussion of the analysis and assessment techniques to be used; and a discussion of system performance metrics including both measures of effectiveness and measures of performance. Phase I should also include the processing and submission of any necessary human subjects use protocols. Phase II plans should also be provided, to include key component technological milestones and plans for testing and validation of the proposed tool and its components.

PHASE II: Develop a prototype tool based on the preliminary design from Phase I. All appropriate pilot testing will be performed, and a critical design review will be performed to finalize the design. Phase II deliverables will include: (1.) a working prototype of the tool, (2) specification for its development, (3) demonstration and validation of ability to assess the workload of a distributed team connected through a network.

PHASE III: This technology will have broad application in military as well as commercial settings. The military has

demonstrated an increase in the need for teams to operate in a distributed manner. Consequently tools that afford leadership the ability to monitor and assess these distributed teams' workload are crucial to ensure that the Warfighter is cognitively ready to conduct required military operations. The commercial sector has also shown an increase in teams that are distributed. The proposed tool should allow managers and team leads to gauge the current and projected workload of their teams allowing them to make essential personnel decisions.

REFERENCES:
[1] Cooke, Salas, Cannon-Bowers, Stout, (2002). "Measuring Team Knowledge." Human Factors, Volume 42.

[2] Donmez, B., Brzezinkski, A.S., Graham, H., Cummings, M. L., (2009). Modified Cooper Harper Scales for Assessing Unmanned Vehicle Displays. Retrieved on September 11, 2009 from: http://halab.mit.edu

[3] Lysaght, R., Hill, S., Dick, A.O., Plaondon, B., Linton, P., Wierwille, W., Zakland, A., Bittner, A., and Wherry, R., (Jun 1989). "Operator Workload: Comprehensive Review and Evaluation of Operator Workload Methodologies."

[4] Hart, Sandra G., (2006). NASA Task Load Index (NASA-TLX); 20 Years Later. Human Factors and Ergonomics Society. (2006).

[5] Hart, S. G. & Staveland, L.E. (1988) Development of NASA-TLX (Task Load Index): Results Of empirical and theoretical research. In P. A. Hancock and N. Meshkati (Eds.) Human Mental Workload. Amsterdam: North Holland Press.

[6] Salas, E., Dickinson, T. L., Converse, S. A., and Tannenbaum, S. I. (992). Toward an understanding of team performance and training. In R. W. Swezey & E. Salas (Eds.), Teams: Their training and performance (pp. 3-29). Norwood, NJ: Ablex.

[7] Urban, J., Bowers, C., Monday, S., and Morgan, B., (1995) "Workload, Team Structure, and Communication in Team Performance." Military Psychology. Volume 7.

[8]Waard, D. de. (2005). The Measurement of Drivers' Mental Workload. Retrieved September 2, 2009 from: http://irs.ub.rug.nl/ppn/297329391

KEYWORDS: Cognitive Readiness, Team Performance, Assessment

OSD10-CR7 TITLE: Improving Team Readiness through the Convergence of Team Mental Models

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: Cognitive readiness (Morrison, 2002) is defined as "the mental preparation (including skills, knowledge, abilities, motivations, and personal dispositions) an individual needs to establish and sustain competent performance in the complex and unpredictable environment of modern military operations". Because teams increasingly play a vital role in networked military operations, it is necessary to expand the notion of individual cognitive readiness to team cognitive readiness through novel representations of a Team Mental Model (TMM). TMMs are defined as "team members' shared, organized understanding and mental representation of knowledge about key elements of a team's relevant environment (goals, assumptions, tasks, etc)", and can be constructed through the analysis of team communication data (audio, chat, etc). However, a key challenge is to elicit and incorporate tacit knowledge into TMMs, because the key factors/variables associated with cognitive readiness (motivations, abilities, etc) may not always be explicitly represented in a team's communication stream. The topic is interested in tools that embed novel conceptual & mathematical representations for TMMs, new techniques that measure the TMM consistency across larger teams and new approaches to enable the alignment of a TMM with the team's beliefs in order to assess and improve a team's cognitive readiness.

DESCRIPTION: The research topic is soliciting tools that embed novel conceptual and mathematical

representations of TMMs, particularly based on new techniques that elicit tacit knowledge associated with cognitive readiness (e.g., motivations, abilities) that can be integrated with a team's communication-based knowledge. Furthermore, due to uncertainty of the environment, or limited availability of information across team members, a TMM may diverge from individual member beliefs. There has been limited research in similarity of shared mental models [Ross, 2007]; however, new similarity metrics that can quantify the divergence across larger teams need to be developed. Based on the level of divergence of the TMM, innovative techniques should be developed to bring the TMM into alignment with the team beliefs.

PHASE I: Develop appropriate conceptual designs for a TMM which include the key factors/variables (motivations, abilities, etc) associated with cognitive readiness.

PHASE II: Develop techniques to elicit tacit knowledge within the conceptual TMM design from Phase 1 and implement an overall mathematical representation of a TMM. The similarity metrics for TMMs should scale to larger teams in accuracy and performance as a function of the number of users, number of interaction modalities, number of models and number of data sources. Based on the degree of similarity, develop techniques to bring the model into alignment with the beliefs of the team. In addition, develop effective visualization techniques to enable an intuitive understanding of the TMM.

PHASE III: Involve subject matter experts in order to test and validate the tool through appropriate experimentation in order to enable transition.

REFERENCES:
[1] Morrison, John E., Fletcher, J.D., "Cognitive Readiness", IDA Paper P-3735, October 2002.

[2] Ross, S., Allen, N., "Examining the Convergent validity of Shared Mental Model Measures", Presented at the INGRoup Conference, East Lansing, MI. July 2007

KEYWORDS: Cognitive Readiness, Team Mental Model, Team Convergence

OSD10-CR8 TITLE: Decision Support: Cognitive Readiness Assessment and Reporting

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: The objective of the topic is to develop a hardware and software solution for both understanding of and augmentation of cognitive readiness at both the individual and command levels.

DESCRIPTION: The U.S. military continues to enjoy significant advantages over our adversaries with respect to our personnel, training techniques, equipment, and emerging technologies. When these systems are combined within an increasingly dynamic and demanding environment, the cognitive capacities of warfighters in theater often become strained to the point where operational effectiveness is diminished. Just as significant research, testing and evaluation, and analysis are conducted to ensure the operational readiness of combat technologies before they are deployed, the individual warfighter and respective Commander need to be able to assess actual 'readiness' of the warfighters for whom these technologies were created. Cognitive readiness is the mental preparation (including skills, knowledge, abilities, motivations, and personal dispositions) an individual needs to establish and sustain competent performance in the complex and unpredictable environment of modern military operations (Morrison & Fletcher, 2001).

With the current emphasis on joint operations and non-kinetic warfare, decreased cognitive readiness will directly affect team cohesion and effectiveness and will limit the warfighters' ability to work within culturally diverse and complex environments, and to build the local relationships and partnerships essential to executing these missions. The criterion for warfighter success can be defined as "fully prepared joint-warfighters fighting and winning in an information-rich, distributed firepower battle space using human-centered hardware and systems." Based on the needs of the military, new developments are needed to enable the cognitive readiness of warfighters. With a better understanding of cognitive readiness, an individual could better handle multiple and complex tasks as well as

understand when their capacity would be expected to be exceeded by task demands.

A new approach to measuring cognitive readiness is needed that can be applied and customized across branches and divisions of the military. One solution involves a hand-held, touch screen device capable of measuring various aspects of individual users' cognitive readiness, augment their readiness, and collate a number of individuals' readiness states in a report to pertinent personnel.

Similar to popular 'smart phone' interfaces of today, a hand-held device and suite of software applications relevant to warfighter cognitive readiness is needed. Cognitive readiness encompasses a number of psychological components, including situation awareness, transfer of training, and decision-making among others (Fletcher, 2004). Example applications may include those that offer refresher training options, sleep and schedule recording, workload measurement, and mission descriptions and warfighter specific tasks. Applications should have the ability to send statistical information to a central software application for review and decision support functionality. An example of a relevant application from previous research is a web-based survey and feedback system developed to improve decision support for leaders in military medical teams (Bolstad, Cuevas, and Costello, 2008). Applications should provide proper feedback, and where applicable inform the individual of their own current cognitive readiness state. Applications may also increase situation awareness by allowing rapid understanding of individuals' statuses displayed in relation to others in a network (e.g. mapping capabilities) and through information sharing between individuals or across a network (e.g. Beale, 2005). Distributed applications created for this environment could be used to update training records; create training schedules; assess problem solving, leadership, mental flexibility and creativity; and determine mission assignments and duty schedules.

PHASE I: Develop a detailed conceptual design for the applicability of a hand-held touch screen hardware/software cognitive readiness solution. Identify potential applications capable of measuring and augmenting cognitive readiness of an individual. Develop a framework for information sharing and data fusion within a network of individuals and across applications. Provide a limited demonstration of the technical feasibility of the conceptual design.

PHASE II: Produce prototype hardware based on Phase I work. Develop, demonstrate and validate several applications which are capable of both measuring and augmenting cognitive readiness. Demonstrate information sharing and data fusion across a network of individuals.

PHASE III: Transition the prototype to fleet-ready equipment.

REFERENCES:
[1] Beale, R. (2005). Supporting social interaction with smart phones. IEEE Pervasive Computing 4(2), 35-41.

[2] Bolstad, C.A., Cuevas, H.M., & Costello, A.M. (2008). Predicting cognitive readiness of deploying military medical teams. In Proceedings of the Human Factors and Ergonomics Society 52nd Annual Meeting, 970-974.

[3] Fletcher, J. D. (2004). Cognitive readiness: Preparing for the unexpected (DTIC No. ADA458683). Alexandria, VA: Institute for Defense Analyses.

[4] Morrison, J.E. & Fletcher, J.D. (2001). Cognitive readiness (IDA Paper P-3735). Alexandria, VA: Institute for Defense Analyses.

KEYWORDS: Cognitive Readiness, Situation Awareness, Decision Augmentation

OSD10-CR9 TITLE: Embeddable Agents for Assessing Cognitive Readiness

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: This effort will develop and demonstrate an embeddable, modular and evolutionary agent technology that can be integrated into existing military systems to collect and analyze cognitive performance data from human

operators using their designated systems.

DESCRIPTION: The military and commercial sectors have devoted considerable resources to developing highly complex operational systems with the goal of significantly improving the performance range of today's warfighter [1]. Yet, with increased complexity comes the risk of increased operator workload, decreased cognitive flexibility and delayed, and even incorrect, action [2,3]. One way of mitigating this cognitive cost would be to develop systems that can support embedded performance assessment and instructional tools [4,5]. However, research advances in the neuroscience of cognition are advancing much faster than the system development lifecycles for any given military technology. As a result, it is not possible to embed the most recent advances in performance assessment into any a priori design decision.

One solution to this challenge is to develop a stand alone capability for monitoring and assessing operators as they use their designated systems to identify performance deficits for training and performance support. This capability would be platform independent and would sit on top of a given system's existing architecture. The system would include the ability to capture system and user performance data which would then be used to develop and/or inform models of operator performance and determine when/if performance support or training is required for mission accomplishment.

This topic will develop an agent-based capability [6,7] that can be seamlessly embedded with existing operational systems to gather operator and equipment data such as baseline operator performance models, performance checklist information and operator/ equipment interaction feedback data, using neural, cognitive and behavioral data sources, as well as equipment generated data sources. Sources of nueral data should be collected using technologies that are non-invasive and minimally intrusive so as to not interfere with user performance. Within the envisoned solutionm, care must be given to ensuring that sensor size, weight and power requirements are minmized and that the total number of sensors used is optimized. This capability must also include the ability to create system- relevant metrics at the individual and team levels, and allow for the identification of the etiology and assessment of performance errors.

PHASE I: Prepare a feasibility study for developing an embedded agent capability that will collect and analyze performance data of human operators engaged in using their designated systems. The performer will propose a conceptual device and a preliminary design/architecture. A final report will be generated, including a detailed description of assessment metrics (measures of performance and measures of effectiveness) and plans for Phase II. Cost-savings from developing this bridge capability will be considered a critical performance metric. Phase II plans should include key component technological milestones and plans for at least one operational test and evaluation using an operational system. Phase 1 should also include the processing and submission of all required human subjects use protocols.

PHASE II: Develop and demonstrate an embeddable, modular and evolutionary agent technology that can be integrated into existing – or under development - military systems to collect and analyze cognitive performance data from human operators using their designated systems, based on the preliminary design from Phase I. All appropriate testing will be performed, and a critical design review will be performed to finalize the prototype specifications.. Phase II deliverables will include: (1) a working prototype of the technology (2) specification for its development, and (3) test data on its performance collected using one or more operational systems.

PHASE III: This technology will have broad application in military as well as commercial settings. Recent advances in cellular phone, personal data assistants and related hand-held computing technologies have demonstrated that powerful and compact communication, data collection, aggregation and analysis systems can be built and interfaced with larger systems, on-demand. Embedding software agent models and procedures in a hand-held technology provides portability such that each user can have a personal data assistant to help them track their specific learning and performance strategies and history. It also provides a mechanism for performance monitoring of users and of specific systems, performance proficiencies with these systems and diagnostic data to identify performance deficits for training and performance support. Commercially, this technology will enable never-before achieved levels of targeted technology support, enabling a third-party approach to rapidly diagnosing user-system problems. For the military and commercial sectors, this technology will provide a novel approach for providing reach-back potential for system maintainers as well as for enabling real-time performance support that can be integrated into online and distributed learning technologies.

REFERENCES:
[1] Scerbo, M.W. (1996). Theoretical perspectives on adaptive automation. In R. Parasuraman & M. Mouloua. (Eds.), Automation and human performance: Theory and applications (pp. 37-63). Mahwah, NJ: Lawrence Erlbaum Associates.

[2] Woods, D. D. (1996). Decomposing automation: Apparent simplicity, real complexity. In R. Parasuraman & M. Mouloua (Eds.), Automation and human performance: Theory and applications (pp. 3-18). Mahwah, NJ: Lawrence Erlbaum Assoc.

[3] Billings, C.E. (1997). Automation aviation. Mahwah, NJ: Lawrence Erlbaum Associates.

[4] Kozlowski, S.W.J., Toney, R.J., Mullins, M.E., Weissbein, D.A., Brown, K.G. & Bell, B.S. (2001) Developing adaptability: A theory for the design of integrated-embedded training systems. In: E. Salas (Ed.) Advances in human performance and cognitive engineering research (Vol. 1, pp. 59-122). Amsterdam: JAI/Elsevier Science.

[5] Cheikes, B.A., Geier, M. et al (1998). Embedded training for complex information systems. In: B.P. Goetl et al (Eds) ITS ’98, LNCS 1452 pp 36-45.

[6] Otsuka, J.L., da Rocha, H.V. (2002) An Agent-Based Approach to Support Formative Assessment, 2002 International Conference on Computers in Education (ICCE '02), pp. 1486.

[7] Cockayne, W. C. & Zyda, M. J. (1997). Mobile Agents Manning Press, Greenwich, CT.

KEYWORDS: Embedded Agent Architecture; Performance Support; Training; Cognition; Assessment

OSD10-C10 TITLE: Real-time Cognitive Readiness Assessment Tool

TECHNOLOGY AREAS: Human Systems

OBJECTIVE: Develop a real-time cognitive readiness tool that utilizes existing data sources and performance models to assess troop readiness levels.

DESCRIPTION: With the current buildup of troops in Afghanistan and the potential for short-term military operations in other remote areas, it is likely that Special Operations forces will be conducting increasing numbers of “quick-strike” missions in hostile areas. Regular units will also likely be increasing the numbers of patrols and convoys throughout these areas. Military planners and field commanders will therefore need instantaneous access to all relevant information to ensure that their troops are fully prepared to conduct these missions. Current databases contain specific information on number and type of occurrences and locations of hostile incidents such as IED explosions in these areas. In addition, information such as satellite maps, terrain information, and other environmental conditions are available through the open literature, as well as models that can predict both physiological and mental fatigue based on parameters such as sleep deprivation, mission qualification, injuries, prior training, and altitude. However, most of these databases and models are not instantaneously available to mission planners and field commanders, and no method currently exists that is capable of accessing multiple sources for evaluating cognitive readiness. Examples of potential data sources include Combined Information Data Network Exchange (CIDNE), Tactical Ground Reporting System (TIGR), Fatigue Avoidance Scheduling Tool (FAST), Altitude Decompression Risk Assessment Computer (ADRAC) model, and National Geospatial-Intelligence Agency (NGA) mapping/terrain data. All these factors influence the readiness of troops to engage and defeat the enemy. This effort proposes a “real-time cognitive readiness tool” that could be used by mission planners and field commanders to instantaneously select and access relevant data sources and models, enter current environmental and troop conditions, interpret the available data, and then use the information to upgrade their troops’ cognitive readiness by presenting them with an assessment of the likely risks to accomplishing their mission. The proposed effort should focus on identifying and processing data sources and models which are both attainable and predictive of troop readiness, provide the user with a means to enter existing field conditions, and then employ innovative

factor weighting and/or data mining techniques to establish statistical correlations among the chosen data sets that would allow the planners to establish the level of cognitive readiness.

PHASE I: Design the concept and evaluate the feasibility of a cognitive readiness tool capable of remotely accessing and displaying existing relevant data sources and models, entering current environmental and troop condition data, and displaying an overall risk assessment of cognitive readiness. Select and give rationale for selection of the data sources and models, describe the proposed methodology for conducting the assessment (statistical factor weighting, Baysian Belief Network, etc.), and provide an illustration of the proposed graphical user interface.

PHASE II: Develop the prototype tool described in Phase 1. Demonstrate with sample data how the applicable data sources and models identified in Phase 1will be incorporated "real-time" into the system, and include a demonstration using the graphical user interface, showing how data will be entered and displayed under a variety of field conditions. Provide details on the software structure and how cost effective it will be to fully implement, operate, and maintain.

PHASE III: Identify commercialization strategies that could be used to ensure operationally sound integration of the system into platforms compatible with the proposed data sources, and for use under a variety of field conditions. Military applications include use by mission planners for assessment of their troops' cognitive readiness, particularly for operations involving ground vehicle, aircraft, or vessel operation in hostile areas. Civilian applications could include use in assessing operator readiness in areas such as air traffic control, ship piloting, commercial and private aircraft, and other public transportation involving the use of potentially dangerous equipment.

REFERENCES:
1. Tactical Ground Reporting System (TIGR) information located at
http://www.darpa.mil/ipto/programs/assist/assist_tigr.asp

2. USASOC News Service posting on Combined Information Data Network Exchange (CIDNE),
http://news.soc.mil/releases/News%20Archive/2006/06FEB/060214-02.html

3. Geospatial-Intelligence Forum "Mapping the Human Terrain," http://www.geospatial-intelligence-forum.com/mgt-archives/107-mgt-2009-volume-7-issue-2/930-mapping-the-human-terrain.html

4. 2005 FAST™ FAST Users Forum, http://novasci.ms11.net

5. Altitude Decompression Sickness Risk Assessment (ADRAC) Model information located at USAF Collaborative Biomechanics Data Network (CBDN), https://biodyn1.wpafb.af.mil/altitude

KEYWORDS: cognitive readiness, risk assessment, databases, performance models, mission planning, real-time

OSD10-EP1 TITLE: Parallel Operation of Compact, Efficient Turbogenerators for Robust Tactical Energy Independence

TECHNOLOGY AREAS: Ground/Sea Vehicles, Battlespace

OBJECTIVE: Enable the electrical outputs of multiple, very compact turbogenerators in the 10-50 kW range to be combined ("paralleled") in order to provide a compact, stable, reliable microgrid capable of providing up to 500 kW.

DESCRIPTION: The focus of this topic is system-level control technology which will allow multiple turbine driven electrical generators to work together synchronously to supply an electrical load larger than any individual unit could provide; this would enable a scaled but functionally identical version of the robust utility grid which supplies electrical power consumers. Tremendous advances have been made in the specific thrust, operating efficiency, and cost of small turbojet engines in the 30-100 lbf class. Costs have been reduced to the extent that some low end products are now successfully marketed to radio controlled aircraft hobbyists. Research is ongoing to develop an

auxiliary power unit (APU) based on this state of the art engine technology; the goal of that development is a relatively fuel efficient 30 kW all-electric-output turbine engine driven APU which will be roughly the size of a loaf of bread. Relevant distinctions between that APU and commercially available microturbines are operating speed and rotor inertia. The ability to parallel (i.e., electrically combine) a collection of these units into a microgrid to generate a larger output power, which is the focus of this topic, is very desirable. This microgrid should have all of the features users expect from the utility grid. Investigations into parallel operation of commercially available microturbines have validated the manufacturers' claims of parallel operation but identified that more technology development may be required for stressing applications. Many publications in the literature describe paralleling distributed generation sources, such as microturbines, by recognizing each as a DC source and paralleling the inverters associated with each source to generate the combined output; for this application an approach based on mechanically paralleling the individual units and then processing the combined AC output is expected to be beneficial. In this case, "mechanically paralleling" is taken to mean that the frequency, magnitude, and phase of each APU's voltage waveform will be maintained in synchronism on a common AC bus by proper control of each distributed APU. It is recognized that the ability to operate this microgrid in parallel with the utility grid brings additional challenges and this topic does not require this ability; it is assumed that the microgrid will operate only in an island mode. Automatic start/stop of individual turogenerators based on load is expected to significantly impact the microgrid efficiency and should be investigated as part of the system level control strategy. The ultimate application of this technology could be stationary, such as in a forward operating base, or mobile in a ground or airborne vehicle and the microgrid could supply one large possibly transient load or distributed loads. The required format of the combined electrical output is undefined at this time. Offerors are strongly encouraged to establish relationships with relevant developers of small microturbines.

PHASE I: Investigate approaches to enable parallel operation of individual 10-50 kW turbogenerators to stably, reliably, and efficiently supply a 100-500 kW electrical microgrid and estimate system level impacts of these approaches. As appropriate, modeling and simulation to guide this research is very strongly encouraged.

PHASE II: Develop and demonstrate technology approaches to the extent allowed by the scope, preferably with an industry partner capable of providing hardware to allow a meaningful demonstration of parallel operation of at least two units. Develop a technology transition and/or insertion plan for future systems and commercial ventures.

PHASE III: Integrate these control technologies into a 100-500 kW microgrid and demonstrate the ability to support a single large transient load as well as distributed loads, and reduce the technologies to a marketable product via licensing or well established relationships with system supplier(s).

PRIVATE SECTOR COMMERCIAL POTENTIAL/DUAL-USE APPLICATIONS: These methods could be applied on several planned military and commercial platforms requiring significant levels of electrical power as well as commercial and military facility microturbine installations.

REFERENCES:

1. "Tom-Thumb turbines power radio-controlled jets", Machine Design, 4 Dec 04 (available through www.machinedesign.com)

2. Basic Electric Machines; Vincent Del Toro, 1990, Prentice Hall ISBN 0-13-060146-2, Section 5-8 for basic information on parallel generator operation.

3. "Behavior of two capstone 30kW microturbines operating in parallel with impedance between them"; Yinger, Robert J.; 2004; http://escholarship.org/uc/item/7sp52570

4. "Microturbine Power Conversion Technology Review"; R. H. Staunton and B. Ozpineci ; 2003; ORNL/TM-2003/74; http://www.ornl.gov/sci/btc/apps/Restructuring/ORNL_TM_2003_74_final1.pdf

5. "Small, Low-cost Turbojet Propulsion System for Miniature Munitions"; Air Force SBIR Impact Sheet; http://www.tdi-engines.com/release/USAF%20SBIR%20Impact.pdf

6. "Concerns Generated by Islanding"; Paul L. Villeneuve; IEEE Power & Energy Magazine; May/June 2004; IEEE 1540-7977/04

KEYWORDS: Power, electrical power, turbine engine, turbogenerator, and turbine engine transient response

OSD10-EP2 TITLE: Rugged, collapsible solar concentration devices to support tactical alternative energy production

TECHNOLOGY AREAS: Ground/Sea Vehicles

OBJECTIVE: The objective of this topic is development of a technology that will enable small tactical operations to take advantage of renewable energy, thereby reducing fuel consumption, reducing operational costs, and reducing the need for logistics fuel resupply.

Concentrated Solar Thermal (CST) solar-to-electric conversion is particularly efficient with a net average annual yield rate ranging between 18 and 23%, higher than any other solar energy system.[1] Accordingly, this is the technology of interest for this topic.

DESCRIPTION: The focus of this topic is development of a tactically-mobile, deployable/stowable solar concentrator for use with solar thermal conversion devices (Stirling, Brayton, TPV, etc.) Given the desire for transportability, ruggedization is a critical part of this topic, potentially spurring the requirement for more robust glass/ceramic materials, or higher UV resistance in polymeric materials.

There are many types of solar collectors (flat plate, parabolic trough, parabolic dish, heliostats, etc.) [2] These collectors are being used world-wide at fixed sites, and their use is expanding. For mobile, tactical military units to capitalize on the advantages of solar thermal energy, development is required to understand the potential for concentrators to operate predictably and efficiently after repeated deployments in a demanding environment. The military environment involves temperature, altitude, and humidity extremes [3], but also includes airborne contaminants (engine emissions and others) that could foul reflective surfaces of a solar collector.

Automated two-axis control for solar tracking is desired for maximum solar energy capture. Automated deployment and stowage of the concentrator is preferred. Alternatively, deployment and stowage may be accomplished by 2 personnel within 15 minutes (objective) or 30 minutes (threshold). Proper alignment and focal accuracy is important for maximizing solar energy capture.

PHASE I: Investigate tactical solar concentrator approaches for a 3-5 kW electric power requirement. A system-level approach should be taken such that various types of collectors and thermal-to-electric converter combinations are considered. Identify the most promising combinations of collectors and thermal-to-electric converters for the intended application herein, and provide supporting data. As appropriate, modeling and simulation to guide this research is very strongly encouraged. The target military platform for the solar collector, thermal-to-electrical converter, and auxiliaries involves mounting onto a Light Tactical Trailer (LTT) and towing by a HMMWV.

PHASE II: Develop and demonstrate technology approaches in a lab environment, and with an industry partner capable of providing hardware to enable meaningful system-level demonstrations of one or more solar collector configurations. Characterize the concentrator's ability to provide the thermal input necessary for power generation, optical accuracy & repeatability, deployment times, size, weight, volume, etc. Develop a technology transition and/or insertion plan for future systems and commercial ventures.

PHASE III: Integrate the most promising solar concentrator technology with a thermal-to-electrical converter and mount on the targeted Light Tactical Trailer or similar platform. Demonstrate the ability to produce 3-5 kW electrical output under peak sunlight conditions in a variety of selected geographical locations. Convert the technologies to a marketable product via licensing or well established relationships with system supplier(s).

PRIVATE SECTOR COMMERCIAL POTENTIAL/DUAL-USE APPLICATIONS:
This technology can be utilized by the mobile construction industry to save fuel costs and reduce emissions. State and local governments could also benefit from this technology for various applications.

REFERENCES:
1. Cavallaro F., Renewable Energy 34 (2009) 1678–1685

2. Kalogirou S. A., Progress in Energy and Combustion Science 30 (2004) 231–295

3. Army Regulation 70-38

4. Shuai Y., et al., Solar Energy 82 (2008) 13–21

5. Grimmer, Derrick P., A comparison of compound parabolic and simple parabolic concentrating solar collectors, Solar Energy, Volume 22, Issue 1, 1979, Pages 21-25

6. D.E. Prapas, B. Norton, S.D. Probert, Optics of parabolic-trough, solar-energy collectors, possessing small concentration ratios, Solar Energy, Volume 39, Issue 6, 1987, Pages 541-550

7. Solar Energy Vol. 57, No. 4, pp. 317-321, 1996

8. Kribus A., et al., Energy Conversion and Management 47 (2006) 3582–3590

KEYWORDS: Renewables, Solar thermal power, Solar concentrator, Solar collector, Power generation, Alternative energy

OSD10-EP3 TITLE: APU Silencing Technology Development

TECHNOLOGY AREAS: Ground/Sea Vehicles

OBJECTIVE: Demonstrate hardware to reduce the acoustic signature of a JP-8 burning internal combustion engine (ICE) powered 10 kW auxiliary power unit (APU) to below the threshold of hearing at a distance of 20 meters.

DESCRIPTION: One of the requirements for Silent Watch - the detection less operation of vehicle electrical and electronic systems while the vehicle is at rest in a forward scouting position - is that the electrical power source be inaudible at a reasonable distance. Idling the propulsion engine for this purpose is wasteful of fuel and generates a large thermal signature in addition to an unacceptable acoustic signature, and modification of the exhaust system to reduce noise sufficiently at idle would comprise engine performance in motion. Batteries have insufficient energy storage to support Silent Watch's duration requirement. APUs seem the logical approach, but in U.S. Army experience to date they have proven too loud. As an example, the diesel APU originally in the nose of the Stryker engine compartment was actually louder than the idling propulsion engine.

Commercial efforts to reduce engine noise focus on reducing passenger compartment noise and vibration and reducing outside noise to acceptable levels, with an acceptable impact on fuel economy and engine back pressure. There is a significant difference between reducing outside noise to acceptable levels and minimizing the audible detection distance, because the threshold of hearing is frequency dependent. In other words, a commercial technology designed to reduce outside noise to acceptable levels can leave a frequency component well above the threshold of hearing at distances unacceptable to the military. Simple repackaging of commercial technology will not meet the military requirement, because the commercial technology addresses the wrong problem. Innovative research is especially needed to cope with the long-distance audible component of ICE engine exhaust without generating an unacceptably large or heavy muffling system.

PHASE I: Design a hardware solution to reduce the frequency-dependent acoustic signature of a 15 to 20 BHP diesel engine to below the threshold hearing (as defined by MIL-STD-1474) at a distance of 20 meters. Perform modeling and simulation to predict the system's performance. Develop 3D CAD models of the hardware solution in sufficient detail to allow first order analysis of vehicle integration configuration. Develop prototype and LRIP cost estimates.

PHASE II: Build and test the hardware solution developed in Phase I. The government will chose which APU to demonstrate the hardware solution on, and perform their own set of field testing in addition to those of the contractor. Field testing will include 360 degree multi-frequency sound analysis at varying distances. If possible, the government will provide the appropriate vehicle with the APU, but testing may be performed on a custom test stand.

PHASE III: Pursue dual-use of the developed hardware solution. There are two areas where the technology development in this SBIR proposal could prove dual-use.

The first would be to support the acceptance of anti-idling solutions using APUs. "Anti-idling" is the term used to describe the legal requirements (driven by environmental regulations) for commercial trucks not to run their propulsion engines overnight in an environmental enforcement zone for hotel services while the operator sleeps in the cab. One anti-idling solution is the use of a low pollution emitting ICE APU. Reducing the audible range of this APU would increase the number of sites the truck operator could overnight in an environmental enforcement zone.

The second would be to support the acceptance of distributed electrical generation. Today"s electrical grid is characterized by a few large-capacity electrical power plants located a long distance from the customers. Distributed electrical generation is the concept of having a greater number of smaller-capacity electrical generators located closer to the customers. Distributed electrical generation promises commercial cost-savings by reducing electrical transmission infrastructure and providing greater overall system reliability. Community acceptance of local generators would be augmented if they were inaudible.

REFERENCES:
1. MIL-STD-1474D (or newest revision), Department of Defense Design Criteria Standard—Noise Limitations, 12 February 1997.

2. General Performance Specification for the Common Modular Power System, Draft Version 0.10, 29 October 2007, (CMPS Perf Spec v10.doc).

KEYWORDS: Active noise control, noise suppression, noise control, NVH, damping, noise reduction, noise mitigation, sound reduction, radiated noise reduction, wave, acoustical modeling, acoustics, sound suppression, noise abatement

OSD10-EP4 TITLE: Near Field Contactless Electric Power Transfer

TECHNOLOGY AREAS: Ground/Sea Vehicles

OBJECTIVE: Demonstrate hardware to wirelessly transfer electrical power on the order of 20 to 75 watts over a distance of 1 to several centimeters.

DESCRIPTION: All conventional electrical power distribution onboard US Army military ground vehicles is performed using insulated copper wires. This distribution technology is robust and mature, but has its limitations. Running power lines to electrical loads added after vehicle design can be inconvenient and sometimes hazardous depending on load positioning and vibration induced chaffing. Loads that move relative to the vehicle’s electrical system cannot be connected easily. Electrical terminal connections can loosen and become intermittent due to vehicle vibration and dirt intrusion.

Development of a technology where power transfer between points is done without the intervention of a physical metallic conductive medium allows physical design solutions forbidden by conventional insulated copper wires. An electrical load whose location on the vehicle is dependent upon mission, such as a sensor, might be quickly relocated without moving conductors or breaking and making new electrical terminal connections. Physical locations currently denied to electrical loads because of the difficulty of running the electrical connection past obstructive geometry could now be used.

PHASE I: Conduct a review and prepare a report on the state-of-the art, feasibility, and military ground vehicle applications of near field contactless electric power transfer technologies. (Known current examples include airline seat entertainment systems, some phone battery chargers, and the electrical charging system of General Motors EV1.) Design and model a system appropriate to military ground vehicles that could transfer 20 to 75 watts across a distance of 1 to several centimeters. Build a laboratory bench top working demonstration unit.

PHASE II: Based on the results of Phase 1, build a near field contactless electrical power transfer unit and demonstrate it in an operating vehicle. The physical conditions the unit is subjected to would at a minimum be light duty passenger vehicle levels of noise, vibration, and harshness (NVH), and preferably military vehicle level NVH.

PHASE III: Pursue dual-use of the developed hardware solution. There are three areas where the technology development in this SBIR proposal could prove dual-use.

The first would be on light duty passenger vehicles, where ability to place loads in currently denied locations and the ability to power movable loads could be a consumer attractive feature.

The second would be on reconfigurable robotic systems presently limited by the twisting / stretching limitations of insulated copper wire.

The third would be in aircraft use, where in addition to the uses already listed, contactless power transfer could be attractive for use in explosive atmospheres such as inside fuel tanks.

REFERENCES:
1. D. A. Pedder, A.D. Brown, “A contactless electrical energy transmission system”, IEEE Trans. on Ind. Electronics, Vol 46, no. 1, Feb, 1989, pp. 23-30.

2. A. W. Kelley, W. R. Owens, “Connectorless power supply for an aircraft-passenger entertainment system”, IEEE Trans. on Power Electronics, vol 4, no, 3, July 1989.

3. P. Knaup, “A method to optimize the size of the transformer core for magnetic power transfer to linear moving devices: PCIM 98.

KEYWORDS: Contactless power, non-contact power, robotic, unmanned vehicle, vehicular power system

OSD10-EP5 TITLE: Redeployable Solar Combined Heat and Power (RSCHP) System

TECHNOLOGY AREAS: Ground/Sea Vehicles

OBJECTIVE: To develop a containerized solar thermal energy collection and generation system that can produce combined heat and power (CHP) for deployable shelter systems and base camp installations.

DESCRIPTION: Deployed forces use engine-driven generators and water heaters that burn millions of gallons of logistics fuel. A RSCHP containerized system would allow for off-grid locations to provide at least a portion their own heat and electricity. This would lower fuel consumption, decrease the number of required refueling, and lessen the need for fuel transportation.

For example, it is estimated that a 50 m2 array RSCHP system could generate at least 100 kWh/day. From this, the estimated JP-8 fuel savings would be about 3300 gallons/year per RSCHP system. If there are roughly 800 Forward Operating Bases (FOBs) and each base had 1 RSCHP, the yearly fuel savings would be 2,640,000 gallons (compared to a roughly 30% efficient 30kW 60Hz TQG JP-8 fueled electrical generator). Calculated savings is for electrical production only; it does not include possible water heating savings.

Although 50 m2 is used as an example, the specific objective is to select and integrate the greatest possible amount of solar energy collection and electrical conversion technology that fits within and can be deployed from a standard

20 foot ISO shipping container. To further maximize the overall efficiency of the system water heating can be integrated. The RSCHP system should be modular, scalable, and interact with other power modules to partially satisfy or supplement the energy requirements of the deployment. Electrical power produced would assist in powering deployable shelters or entire camps, including lighting, Environmental Control Units (ECU), and Command & Control equipment. A RSCHP system could be a key contributor to a microgrid system which would store and efficiently manage energy from multiple input sources.

Most solar energy systems that are commercially available are designed for stationary permanent public utility applications. Scaling these systems for portable deployable military applications is the primary challenge. Concept systems can utilize or combine any form of solar energy collection (e.g., trough, Fresnel, heliostat) and any form of solar thermal power generation (e.g., organic Rankine cycle, sterling cycle). It is desired that RSCHP not use conventional generators for deployment or start-up.

Emphasis should be placed on energy conversion efficiency (sun to electricity), energy storage capabilities, and energy produced per unit area of solar collector (kW/m2/day). The main focus of this project is to produce the maximum amount of solar generated electrical power in a package restriction, or cube, of a single 20'x 8'x 8' standard ISO/CONEX container. The deployable components must be man-portable (the MIL-STD-1472 limit for a 4 person "lift and carry" is 147 pounds) and this requirement and the dimensions of the container will determine the actual area and quantity of the individual collectors. The collectors can be rigid or flexible, troughs or flat, sun tracking or fixed, whichever combination minimizes the cube, weight, and cost, and provides adequate reliability and ruggedness for field applications. The container must include all of the system components. An additional desired specification to be met is the exit hot water temperature. If a solar thermal systems waste heat is used to heat water, the water must be able to reach temperatures of 150o F.

PHASE I: Research, develop, and design an innovative concept with detailed and quantified arguments for feasibility. Comparisons should be made to present-day technology, as well as other similar applications. A major deliverable required in Phase I will be a detailed prototype system design which outlines the solar collection method, energy conversion/generation techniques, system configuration, deployment method, and energy storage abilities (ex. batteries, molten salt). The prototype design must be supported by credible data showing that the system could provide the proposed output values. Any prediction modeling, calculations, or working examples that can validate the systems feasibility and performance potential should be provided. The hardware deliverable for Phase I will be a small scale (1-2 collectors, plus power generation system) proof-of-concept model validating each technology of the designed system. This includes demonstrating 120V AC electrical production (w/ storage) and potential water heating ability. Deliver a final report specifying how full-scale performance and control requirements will be met in Phase II. The report shall also detail the conceptual design, performance modeling, safety, risk mitigation measures, MANPRINT, and estimated production costs.

PHASE II: Refine the concept and fabricate a full scale prototype containerized RSCHP that is transportable and deployable, meets electrical power and hot water predictions from phase I, and is sufficiently mature for technical and operational testing, limited field-testing, demonstration, and display. Define manufacturability issues related to full scale production of the prototype system for military and commercial application. Identify safety and human factors and provide user manuals and training to support testing of the equipment.

PHASE III DUAL USE APPLICATIONS:
The initial use for this technology will be to provide electrical power and hot water for military base camp organizational systems. Solar electric and heat is applicable to both military and civilian markets. The Army Strategic Action Plan for Sustainability includes objectives, measures and targets for fuel reduction (30% by 2020). The Army Energy Security Implementation Strategy also has several fuel objectives including: "Objective 2.6 Increase energy efficiency of current and tactical equipment/platforms". There are also initiatives for Zero-footprint Base Camp, the NetZero Plus Joint Concept Capability Technology Demonstration, and the Force Provider Environmental Technologies Working Group, all of which focus on technology to reduce fuel and water consumption. There are also tax incentives for alternative and renewable energy for home owners and businesses.

REFERENCES:
1. "NREL: Concentrating Solar Power Research - Publications." National Renewable Energy Laboratory (NREL). Web. 15 Sept. 2009. http://www.nrel.gov/csp/publications.html.

2. "NREL: Distributed Thermal Energy Technologies - Combined Heat and Power." National Renewable Energy Laboratory (NREL) Home Page. Web. 15 Sept. 2009. http://www.nrel.gov/dtet/heat_power.html.

3. “Advances in solar thermal electricity technology” by D. Mills, Solar Energy, Volume 76, Issues 1-3, January-March 2004, Pages 19-31, Solar World Congress 2001. Available on ScienceDirect.com

4. “Design and thermal analysis of a two stage solar concentrator for combined heat and thermoelectric power generation” by Siddig A. Omer and David G. Infield, Energy Conversion and Management, Volume 41, Issue 7, May 2000, Pages 737-756. Available on ScienceDirect.com

5. “A combined heat and power system for buildings driven by solar energy and gas” by A. C. Oliveira, C. Afonso, J. Matos, S. Riffat, M. Nguyen and P. Doherty, Applied Thermal Engineering, Volume 22, Issue 6, April 2002, Pages 587-593. Available on ScienceDirect.com

6. “Solar energy powered Rankine cycle using supercritical CO2” by H. Yamaguchi, X.R. Zhang, K. Fujima, M. Enomoto and N. Sawada, Applied Thermal Engineering, Volume 26, Issues 17-18, December 2006, Pages 2345-2354. Available on ScienceDirect.com

7. “Micro-combined heat and power in residential and light commercial applications” by M. Dentice d’Accadia, M. Sasso, S. Sibilio and L. Vanoli, Applied Thermal Engineering, Volume 23, Issue 10, July 2003, Pages 1247-1259. Available on ScienceDirect.com

8. United States. U.S. Army. Office of the Deputy Assistant Secretary of the Army for Energy and Partnerships. ARMY ENERGY SECURITY IMPLEMENTATION STRATEGY. U.S. Army, 13 Jan. 2009. Web. http://www.asaie.army.mil/Public/Partnerships/doc/AESIS_13JAN09_Approved%204-03-09.pdf

KEYWORDS: combined heat and power, solar energy, renewable energy, power generation, water heating, off-grid, remote

OSD10-EP6 TITLE: Anion Exchange Membranes for Alkaline and Low-temperature Fuel Cell Applications

TECHNOLOGY AREAS: Ground/Sea Vehicles

OBJECTIVE: Investigate anion exchange membranes for alkaline and low temperature fuel cell applications.

DESCRIPTION: Anion exchange membranes have the potential to not only improve the performance of alkaline and low-temperature fuel cells, but also reduce the cost and use of precious metal catalysts. These types of membranes would reduce/eliminate osmotic drag and reduce crossover of fuel and other reactants from anode to cathode.

Anion exchange membranes are seen as key enabling technologies for the development of a liquid-liquid fuel cell for underwater applications. In particular the sodium borohydride-hydrogen peroxide fuel cell, the hydrogen peroxide (as the oxidant) is directly electrochemically reduced in an acid electrolyte and the borohydride is direct electrochemically oxidized in an alkaline electrolyte. The anion exchange membrane would enable the conduction of hydroxide ions generated at the cathode to migrate to the anode to participate in the oxidation reaction minimizing the amount of caustic required to be stored as part of the fuel. The weight/volume of these underwater systems are critical and any time the reactants can be reduced/minimized will only improve system efficiency.

Improvements are needed in the anion exchange membranes to be viable for fuel cell applications; these include, improvements in conductivity, robustness and membrane durability. These membranes must be tolerant of simultaneous exposure to alkaline and acid electrolyte; wherein concentration could range between 0.5 to 5 M for each electrolyte over a temperature range of 0 to 80oC.

PHASE I: The contractor will develop a series of membranes that will exhibit some of the following properties: membrane thickness <200um with ionic conductivity of OH- of >0.1S/cm. The contractor will have also characterized the membrane to show electro-osmotic drag coefficient, lambda values, and crossover of other target molecules that could be present in the electrolyte solutions. Membrane characteristics should be recoverable after dehydration which would simulate a period of time where in the future fuel cell may lay dormant in storage. The membrane will also be evaluated in a fuel cell showing both polarization profile and constant current performance.

PHASE II: The contractor will focus on membrane improvements and demonstrate scalability (at least 12”x12” sizes). Membrane should demonstrate minimum 500 hours of constant current performance and restart after a period of dormancy.

PHASE III: The contractor will demonstrate the optimized anion exchange membrane in a multi-cell/stack configuration and test the stack for endurances of 100 hours with multi starts with performance efficiencies of at least 60% utilization.

REFERENCES:
1. Improved Performance of Alkaline Membrane Fuel Cells based on Newly Developed Electrolyte Materials, H. Yanagi et al, 216th ECS Meeting, Vienna, October 2009.

2. Polymeric Membranes for Direct Borohydride Fuel Cells: a comparative Study, D.M. Santos, et al, 216th ECS Meeting, Vienna, October 2009.

3. Direct Borohydride Fuel Cell Development, R. Jamard, Vienna, October 2009.

4. Alkaline Membrane Electrolyte Fuel Cell Research and Development at the US Army Research Laboratory, D. Chu, 216th ECS Meeting, Vienna, October 2009.

5. A novel anion exchange membrane for alkaline fuel cells, Y. Luo, 216th ECS Meeting, Vienna, October 2009.

6. Air Independent Fuel Cells Utilizing Borohydride and Hydrogen Peroxide, R. Craig Urian Materials Research Society Fall Meeting, Boston MA, November 2009.

KEYWORDS: anion exchange membranes, hydrogen peroxide, sodium borohydride, alkaline fuel cells, low-temperature fuel cells, UUVs

OSD10-EP7 TITLE: Advanced System-Level Integration for High Efficiency Primary and Secondary (Waste Heat) Thermoelectric Generation

TECHNOLOGY AREAS: Ground/Sea Vehicles

OBJECTIVE: Develop integrated, high system-level-efficient technology for conversion of thermal energy (from primary fuel or high grade secondary waste heat) to electricity that can be customized for applications from warfighter-portable power to reduce mission load, to fuel-efficiency improvement on military platforms, leveraging state-of-the-art thermoelectric, heat exchange, and power conditioning technologies.

DESCRIPTION: Energy efficiency and mission load are critical challenges for the U.S. military from the individual warfighter to stationary and mobile platforms. The ability to convert thermal energy to usable electrical power with high system-level efficiencies has the potential, depending on the source, to improve the military’s fuel efficiency, mission flexibility and load, and energy sustainability. This program focuses on developing new concepts for high system-level efficiency thermoelectric conversion thermal energy, whether from primary fuel sources (e.g., JP-8, local biofuels, et al.) or high grade opportunistic sources (e.g., waste heat from engines, generators, et al.) to electricity with a focus on efficient integration of state-of-the-art thermoelectric materials/modules, heat transfer technologies, low-parasitic interfaces, and low overhead power conditioning electronics. The significant advances in

the intrinsic conversion efficiencies in thermoelectric materials over the last decade have yet to be translated to increases in system-level efficiencies. To achieve system-level efficiencies, improvements are needed for low parasitic thermal, electrical, and mechanical integration, as well as low overhead power conditioning and load matching to produce usable power for mobile force applications such as battery recharging and fuel-flexible operation of mobile electronics. The objective is to develop a temperature- and power-scalable TEG for both opportunistic thermal energy harvesting and fuel-flexible heat source at the 100W level with system-level efficiency target of 30% of Carnot efficiency with a target external system-level temperature difference of 500C with a cold-side temperature near ambient (25-50C), and power density of 200W/kg.

PHASE I: Develop detailed plans for an integrated thermoelectric generator system incorporating state-of-the-art TE materials/modules, advanced heat exchanger an low parasitic interface technologies, and appropriate power conditioning for scalable 100W power at 14VDC applicable for primary or secondary heat source with a target external system-level temperature difference of 500C with a cold-side temperature near ambient (25-50C). Demonstrate initial scalable system proof-of-concept for overall system-level efficiencies above 30% of Carnot efficiency.

PHASE II: Develop and fabricate a scalable 100W performance- and weight-optimized (200W/kg) integrated thermoelectric generator system suitable for primary (e.g., JP-8 fuel combustion) or secondary (high grade waste heat) thermal source, to be selected by the proposer in Phase I proposal, with appropriate power conditioning that can be integrated into commercial storage system for prolonged sustainable power generation.

DUAL USE COMMERCIALIZATION POTENTIAL: Military application: Military applications for the thermoelectric opportunistic thermal energy harvester/generator include battery recharging and fuel-flexible primary power for electronic equipment.

Commercial application: Commercial applications include but are not limited to waste heat recuperation from commercial and domestic equipment/operations for increased energy efficiency.

REFERENCES:
1. Papers from the International Conf. on Thermoelectrics 2008, J. Electronic Materials, vol. 38 (7), 2009.

2. Rowe, D.M., Ed., “Thermoelectrics Handbook, Macro to Nano”, CRC Press, Boca Raton, FL, 2006.

3. Rowe, D.M., Ed., “Handbook of Thermoelectrics”, CRC Press, Boca Raton, FL, 1994.

KEYWORDS: Energy Harvesting, Fuel Efficiency, Thermoelectrics, Heat Exchanger, Waste Heat Recuperation

OSD10-EP8 TITLE: Magnetic Gears and Couplings

TECHNOLOGY AREAS: Ground/Sea Vehicles

OBJECTIVE: The objective of this topic is to conceptualize, develop, design, prototype and evaluate a quiet, maintenance-free, high torque density magnetic gear and coupling for Navy, DoD, and industrial applications. Mechanical gears require lubrication and maintenance. Magnetic gearing has the potential to be maintenance-free. This alone is reason to pursue development of magnetic gearing for propulsion, power generation, and actuation.

DESCRIPTION: The transition to all-electric combatant ships requires S&T investments in many areas. No Navy or DoD investment has been made in the development of magnetic gearing technology. Early academic/industrial attempts at magnetic gearing involved topologies and materials incapable of providing high-torque levels needed in many industrial applications. With the availability of high-temperature permanent magnet materials and, more recently, soft-magnetic composite materials, there is reason to consider the ability of magnetic gears to offer an alternative to mechanical gears and couplings in some navy applications. With modern magnetics software, multiple topologies can be analyzed quickly enabling near optimal configurations for a given application.

Potential benefits of magnetic gears over mechanical gears involve inherent overload protection through torque shear, elimination of wear surfaces, elimination of the need for grease and lubricants, long-life, high efficiency, and reduced acoustic noise. The potential for low noise alone is an area of interest for the navy's combatant fleet, including UXVs. Actuator motors for control surfaces, in particular, may benefit from this technology. Similar benefits could be applied toward some propulsion and generator drives.

The referenced literature suggests that magnetic gearing R&D has been limited over the past 30 years, but there has been progress in improving efficiency and torque density. Noise performance has not been evaluated. Previous work has been primarily accomplished in Japan, Denmark (University College of Aarhus and Aalborg University), and the UK (Sheffield Univ.), though there is some emerging academic interest in the US. As for technology pull, the NGIPS roadmap and the Navy's UUV Master Plan both call for reduced ship signatures, a potential capability offered by this topic. Some of the key objectives of the NGIPS roadmap relative to this SBIR topic are:

- Increased technology readiness levels
- Decreased system cost / life cycle cost
- Improved reliability / survivability / continuity of service
- Reduced signature for improved "Stealth"

PHASE I: Conduct a scientific study of multiple magnetic gearing and coupling concepts, and identify those most likely to add value to Navy applications. The study shall include predictive performance data in the areas of torque capability, torque density, potential for maintenance-free operation, size, weight, cost, magnetic materials & topology, thermal analysis, etc. Preliminary designs for a magnetic gear and magnetic coupling shall be developed. A final report shall detailing the phase I effort shall be provided.

PHASE II: Based on preliminary designs from phase I, additional analyses / modeling shall be conducted to develop detailed designs for a magnetic gear and a magnetic coupling. Both devices shall be fabricated and performance shall be characterized in the areas of torque capability, torque density (N-m/L, and N-m/kg), efficiency, torque ripple, noise, and overall size and weight at a minimum. In addition to design, development, and testing in this phase, a business case analysis shall be prepared. This BCA shall address life-cycle cost implications of implementing magnetic gears and couplings on existing ships, and on future ships. A final report shall detailing the phase II effort shall be provided.

PHASE III: This effort will result in a magnetic gear and a magnetic coupling at a Technology Readiness Level (TRL) of 6 by 2013. This fits well with the Next Generation Integrated Power System (NGIPS) Technology Development Roadmap. NGIPS incorporates a "Deadline B - 2014", the date when TRL 6 technologies are needed to support forward fit of technology into submarines and potentially later, 2nd generation CG(X). A follow-on opportunity for transition is "Deadline C - 2018", the date when TRL 6 technologies are needed to support new design amphibious warfare ships, auxiliary ships, DDG(X) and a future new design SSN.

The SBIR products (magnetic gear and magnetic coupling) also may lend themselves to transition/implementation on-board existing Navy ships. This decision would depend, in part, on the results of the phase II business case analysis because the up-front cost of retrofitting would need to be considered.

PRIVATE SECTOR COMMERCIAL POTENTIAL/DUAL-USE APPLICATIONS: The industries that may benefit are those currently employing mechanical gearing and couplings for long-term commercial use. Examples include the electric power industry, commercial ship manufacturing industry, and the aircraft manufacturing industry. The potential for application in the automotive and consumer-centric industries will be influenced less by life-cycle costs than by initial purchase price. The business case analysis conducted in phase II will provide detailed information on the anticipated production costs of the devices.

Magnetic transmissions for automobiles and heavy-duty trucks could be an adaptation of this technology in the commercial sector.

REFERENCES:

1. NGIPS Technology Development Roadmap, available:
https://www.neco.navy.mil/synopsis_file/N00024NGIPS_Technology_Dev_Roadmap_final_Distro_A.pdf

2. Naval S&T Strategy, available: http://www.onr.navy.mil/about/docs/0904_naval_st_strategy.pdf

3. H. Toliyat, Gearing Ratios of a Magnetic Gear for Marine Applications, Proceedings of the IEEE Electric Ship Technologies Symposium, 2009

4. Frank T. Jørgensen, Torben Ole Andersen, and Peter Omand Rasmussen, The cycloid permanent magnetic gear, IEEE Transactions on Industry Applications, vol. 44, No. 6, November/December, 2008

5. K. T. Chau, Dong Zhang, J. Z. Jiang, and Linni Jian, Transient analysis of coaxial magnetic gears using finite element comodeling, Journal of Applied Physics vol. 103, January, 2008

6. S. Mezani, K. Atallah, D. Howe, A high-performance axial-field magnetic gear, Journal of Applied Physics 99, 2006

7. K. Atallah, J. Wang, and D. Howe, A high-performance linear magnetic gear, Journal of Applied Physics 97, 2005

8. Kais Atallah, Stuart D. Calverley, David Howe, High-performance magnetic gears, Journal of Magnetism and Magnetic Materials vols. 272–276 (2004) 1727–1729

9. K. Atallah, D. Howe, A novel high-performance magnetic gear, IEEE Trans. Magn. 37 (2001) 2844.

10. K. Tsurumoto, S. Kikushi, A new magnetic gear using permanent magnet, IEEE Trans. Magn. 23 (1987) 3622.

11. D.E. Hesmondhalgh, D. Tipping, A multielement magnetic gear, IEE PROCEEDINGS, Vol. 127, Pt. B, No. 3, May 1980.

KEYWORDS: Magnetics, permanent magnet, torque density, gear

OSD10-HS1 TITLE: Decision Superiority through Enhanced Cultural Intelligence Forecasting

TECHNOLOGY AREAS: Human Systems

OBJECTIVE: The objective of this topic is to develop automated decision aids for the human processing of social-cultural information from large, uncertain datasets to improve time critical decision making in tactical military and interagency contexts.

DESCRIPTION: Social-cultural data is increasingly available to tactical command staffs from a variety of human and unmanned sensors and open source online sites. The enormity of these datasets and the uncertain nature of many data elements are beyond the human analyst's ability to process these data in a timely fashion with the prerequisite level of certainty for decision making. A number of automated decision aiding capabilities have been examined that show promise for future decision support tools. In video surveillance conditions, automated alerts of threatening behaviors based on inputs from multiple collaborating sensors may be promising [1]. Cognitively-inspired decision agents may support the delivery of relevant information to decision makers based on preset decision parameters [2]. Multi-modal information exchange, using a combination of visual, auditory, and touch sensory alerts may also be valuable in extracting information from large data sources [3]. However, there is much to be learned in terms of understanding how humans process and reason about large amounts of data [4] and also how to computationally handle aspects of uncertainty in the data and how to present uncertain data to human users [5].

Research in this area should focus on user requirements for processing information and relationships in large data sets; this knowledge will enable the development of automated decision aids specifically geared toward mission tasks. User requirements should be defined in terms of functionality and performance, requiring a combination of quantitative and qualitative descriptions [6].

Several critical challenges have impeded the design of real-time decision-aiding tools that deal with cultural factors. The first is providing visualizations of complex network and relational data in a form that is readily applicable to mission planning processes. Additionally, unlike some other forms of intelligence data, the cultural data has high levels of uncertainty and data sets often have gaps that may impact the ability of the software decision-aid agent to handle the inconsistencies in the data. Finally, the ability to develop decision-aiding tools that allow real-time knowledge generation are difficult because the predictions are based on correlations between attitudes, influence, and behaviors of political, social, and religious factions in the society. The interactions between these factors can be difficult to understand, model, and predict.

However, military planners and decision makers require access to decision-aiding capabilities of socio-cultural models, as well as the ability to correctly interpret model outputs. As a result, the development of decision aids would greatly assist military planners when using these models. Possible features of the decision aids might include: 1.) better ways to visualize data inputs and model outputs; 2.) provide the ability to easily compare various courses of action; 3.) effectively communicate the uncertainty underlying modeling forecasts; 4.) demonstrate how that uncertainty might impact the selection of particular courses of action; and 5.) highlight gaps in available data that reduce the reliability of forecasts, and offer suggestions about how those gaps might be minimized through the collection of additional data, possibly of a different type.

Challenges for this topic include 1) identifying relevant data sets that provide sufficient sociocultural information to develop models, 2) developing methods to extract features associated with social influence in groups, 3) defining and testing metrics for describing temporal aspects of social network behavior, 4) identifying methods to predict novel concepts that arise from social behavior and attitudes, and 5) the creation of decision aids to translate model outputs into a form that can be more readily used by military planners and decision makers.

PHASE I: Define requirements for a decision-aiding tool that would incorporate a sociocultural database for a population of interest. Identify user requirements for such a tool. Prepare a proof of concept use case for how sociocultural data would be developed, modeled, and presented in a software application for use by military users. Prepare a report documenting methods, theoretical approaches, user requirements, and software applications.

PHASE II: Develop a software application that uses sociocultural modeling and decision-aiding for a population of interest. Utilize one or more established and vetted data sets in this process. Demonstrate visual application of decision-aiding. The prototype should lead to a demonstration of the capability. Test the prototype in an environment to demonstrate feasibility. Propose a verification and validation process.

PHASE III: Produce a system capable of deployment in an operational setting of interest. Test the system in an operational setting in a stand-alone mode or as a component of a larger system. The work should focus on capability required to achieve transition to a program of record or one or more of the military Services. The system should provide metrics for performance assessment.

REFERENCES:

[1] Waskiewicz, T. & LaMonica, P. (2008). Developing an intelligence analysis process through social network analysis. In M. Blowers and Alex F. Sisti, Eds., Evolutionary and Bio-Inspired Computation: Theory and Applications II, Proceedings of SPIE Vol. 6964, 69640B.

[2] Kahn, M. U. & Khan, S. A. (2009). Social networks identification and analysis using call detail records. ACM: ICIS, November 24-26, Seoul, Korea.

[3] Zhang, Y. & Zhao, J. (2009). Social network analysis on data diffusion in delay tolerant networks. ACM: Proceedings of MobiHoc 09, May 18-21, New Orleans, LA.

[4] Drozdova, K. & Samoilov, M. (2009). Predictive analysis of concealed social network activities based on communication technology choices: Early-warning detection of attack signals from terrorist organizations. Computational Math Organizational Theory, DOI 10.1007/s10588-009-9058-2.

[5] Center for Army Lessons Learned. Agribusiness Development Teams (ADT) in Afghanistan Handbook 10-10 Nov 2009, Chapter 6. Available on the web at: http://usacac.army.mil/CAC2/CALL/docs/10-10/ch-6.asp

[6] Stitts, K. B., Phillips, C. L., & Geddes, N. D. (2009). Validation of sociocultural models and meta-models via serious games. IEEE, 5/09.

KEYWORDS: large sociocultural data sets, decision-aiding, user requirements, visualization, socio-cultural awareness.

OSD10-HS2 TITLE: In Situ Collection of Human Social Cultural Behavioral Data

TECHNOLOGY AREAS: Human Systems

OBJECTIVE: The objective of this topic is to develop novel technologies for collecting, storing and making available Human Social Cultural Behavior (HSCB) data for use in both HSCB model verification and validation and in HSCB applications for decision making and course of action development.

DESCRIPTION: With the increasing emphasis placed on non-kinetic, asymmetric and sustainability operations, a growing emphasis is placed on modeling dynamic and complex human social cultural behavior in order to project the consequences of intended actions [1]. These models are only as refined as the data that is provided to them. Today, these models use available HSCB data sets, [2] in order to understand a given population's organization, modes of communication, behavioral trends and such.

Unfortunately, these data sets are limited in number and scope due to the complex and lengthy processes required to populate them. As human behavior is continuously modified though ever changing aspects of the environment, family relationships, and cultural activity [3], HSCB data sets can quickly become out of date or inaccurate. Time constraints and the need for "instant analysis" have increasingly exposed the limitations of traditional SME based analysis and the capabilities of current HSCB analysis frameworks [4]. Lack of current HSCB data availability and flexibility poses significant challenges to understanding and forecasting human activity. Models are limited in their ability to test additional theories and perform verification and validation. As a result, it is difficult if not impossible to effectively utilize current HSCB data sets for novel investigations, often requiring the creation of a unique data set for each novel effort.

The focus of this topic is on developing the capability for long term, sustained data collection technologies from cultural and social regions of interest. The desired data collection capability would include: processes that incorporate techniques to pull in unfiltered data at the source from areas such as multimedia (e.g. Web, television, radio), online record storage, and individual inputs; techniques for representing these data in a standardized, searchable format; and tool sets for visualizing and analyzing these data. Additionally the proposed capability should be able to work in an untended manner, for prolonged durations and include a remote operation capability in order to sustain long-term data collection efforts. Potential Solution types may be either software based, hardware based or both. Proposals should be explicit in indicating what type of solution they will provide at project end, and this must be included as part of the Phase 1 feasibility study, proposed system specifications and preliminary design/architecture.

PHASE I: Prepare a feasibility study for developing novel technologies for collecting, storing and making available Human Social Cultural Behavior (HSCB) data for use in both HSCB model verification and validation and in HSCB applications for decision making and course of action development. The performer will propose a system specifications and a preliminary design/architecture that: a) pull in unfiltered data at the source; b) represents these data in a standardized, searchable format; c) provides tool sets for visualizing and analyzing these data; d) is able to work in an untended manner, for prolonged durations and, e) includes a remote operation capability in order to sustain long-term data collection efforts. A final report will be generated, including plans for Phase II, such as: key component technological milestones, and plans for at least one operational test and evaluation using an operational system. Phase 1 should also include the processing and submission of all required human subjects use protocols if required for Phase II.

PHASE II: Develop and demonstrate technologies for collecting, storing and making available Human Social

Cultural Behavior (HSCB) data for use in HSCB modeling applications, based on the preliminary design from Phase I. All appropriate testing will be performed, and a critical design review will be performed to finalize the prototype specifications. Phase II deliverables will include: (1) a working prototype of the technology (2) specification for its development, and (3) test data on its performance collected using one or more operational systems.

PHASE III: This technology will have broad applications in military as well as commercial settings. Military applications of this technology include enabling commander level officers' rapid, un-biased information regarding target-population dynamics, hierarchies and likely behavioral response to a wide array of interventions in order to help inform their decisions. This technology may also extend beyond commander level officers providing insight to any level of the military that has direct interaction or working with the target population. Commercial applications include domains where personnel with different social – cultural backgrounds must continually interact in dynamic situations where the probability of miscommunication is high and the risk and consequences, great and the need for up to the minute data sets remains unmet.

REFERENCES:
[1] Military Missions and how IOS models can help. (2008). From: Behavioral Modeling and Simulation: From Individuals to Societies. Eds. Greg L. Zacharias, Jean MacMillan, and Susan B. Van Hernel; Committee on Organizational Modeling: From Individuals to Societies, National Research Council.
http://www.nap.edu/openbook.php?record_id=12169&page=23

[2] The DTIC Review: Human, Social, Cultural and Behavior Modeling (2008). Defense Technical Information Center, Fort Belvoir VA: Volume 9, Number 1.

[3] Triandis, H.C. (1989). The self and social behavior in differing cultural contexts. Psychological Review. 96(3): 506-520.

[4] Russell A., and Clark M. (2009). Modeling Human, Social, Cultural or Behavioral Events for Real World Applications: Results and Implications from the State Stability Project. International Conference on Computational Science and Engineering. Vancouver, Canada. ISBN: 978-0-7695-3823-5 August 29-31. DOI Bookmark: http://doi.ieeecomputersociety.org/10.1109/CSE.2009.410

KEYWORDS: Social, Cultural, Behavioral, Modeling, Data Collection, Architecture

OSD10-HS3 TITLE: Neuromorphic Models of Human Social Cultural Behavior (HSCB)

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: The objective of this topic is to develop techniques for modeling human cognition using neural signals that drive human cognitive processes, instead of observed behaviors that result from cognitive processes.

DESCRIPTION: To handle today's complex military environments we must make our warfighters as cognitively strong as they are physically strong. The key to doing this is to accurately model cognition. Human Social Cultural Behavioral (HSCB) models provide an important technology for decision makers at all levels to understand the impact that their actions can have on the mission at hand [1]. The predicted outcomes of these models are only as good as the fidelity of the human behavior representations (HBR) that form them [2]. Often, these models have poor fidelity due to factors that were not included in the original model that may impact the overall behavioral response; these factors include but are not limited to: fatigue, stress, cognitive overload, and changes in context.

Human behavior is the result of the brain's cognitive processes [5]. Cognition is the interaction & integration of 'building blocks' like perception, attention & memory which is how the brain makes sense of information. Each of these building blocks results from activity across multiple brain regions forming 'ad hoc' networks across the physical substrate of the brain [6]. Current cognitive models are based on observed human behavior and do not account for the functions of the brain that give rise to actual human cognition [3]. Traditionally, these models are based on high level representations of individual or aggregate human behavior [4]. Even the best models don't

precisely represent these actions – let alone, cognition because they ignore the brain. Because these representations provide only a snapshot of behavior, when they are included in HSCB models they produce predictions and simulations that are limited to specific activities in a given context.

The focus of this topic is on developing the tools and technologies to create higher resolution and more dynamic representations of human behavior, by including neurally-based representations of human cognitive processes. Current neuroimaging techniques provide the ability to identify individual cognitive processes as they arise, and recent advances in signal analysis technologies provide the means to quickly and accurately decode these processes [7]. These processes can be analyzed in terms of temporal measures (eg how long a "neural circuit" is active), in terms of spatial measures (eg which regions of the brain are active or co-active during the process) or both. Once identified and decoded, these processes could be modeled to understand their impact on alternate cognitive processes that may co-occur during a given military mission. These models would provide the needed fidelity by including the ability to model behavior in a wider array of cognitive situations and alternate contexts. Potential metrics by which to assess model improvement include, but are not limited to: speed metrics (how quickly the model arrives at a solution); accuracy metrics (how close to correct the model solution is); convergence metrics (how closely the model"s speed and accuracy measures reflect actual human performance); comparison metrics (neurocognitive based model perofrmance compared to traditionally developed models); and, completion metrics (how much of what is currently known about the neural action underlying a given cognitive process is captured by the model). Additionally, it is very likely that choice or specific metric set will depend on the chosen task that will be modeled - this choice together with the actual metrics should be clearly identified during Phase 1 and provided in appropriate Phase 1 reports.

PHASE I: Develop requirements specifications for a cognitive modeling technology based on neural signals that drive human cognitive processes, rather than observed behaviors that result from cognitive processes. At a minimum, these specifications must describe: a) how these neural signatures will be collected and validated; b) how these signals will be decoded, and verified, c) how these decoded signals will be modeled and, d) how the model so created will be implemented with an HSCB application. A final report will be generated, including metrics and plans for Phase II. Metrics shall include both measures of effectiveness and measures of performance. Phase II plans should include key component technological milestones and plans for at least one operational test and evaluation and should discuss any interoperability issues likely to be encountered when "porting" a model created on one platform (or for one task or for one person) to another. Phase I should also include the processing and submission of any necessary human subjects use protocols, if required.

PHASE II: Develop at least one complete model of a cognitive process and demonstrate its ability to significantly improve performance of specified HSCB application, based on the preliminary requirements and designs from Phase I. All appropriate engineering testing will be performed, and a critical design review will be performed to finalize the design. Phase II deliverables will include: (1.) a working prototype of the system, (2) specification for its development, and (3) test data on its performance..

PHASE III: This technology will have broad applications in military as well as commercial settings. Military applications of this technology include enabling more effective modeling, simulation and wargaming for the purposes of making more accurate forecasts concerning mission outcomes. As well, cognitive models form the cornerstone for decision support tools, training technologies and human factors/systems design tools. More accurate models of human cognition will enable more effective decision making, improved training and better designed systems, directly supporting mandates to reduce manning while maintaining or improving overall combat readiness. These benefits cut across to commercial applications for this capability including: training and education, entertainment/gaming, and manufacturing/design – any application in which cognitive models form an integral component.

REFERENCES:

[1] Military Missions and how IOS models can help. (2008). From: Behavioral Modeling and Simulation: From Individuals to Societies. Eds. Greg L. Zacharias, Jean MacMillan, and Susan B. Van Hernel; Committee on Organizational Modeling: From Individuals to Societies, National Research Council. http://www.nap.edu/openbook.php?record_id=12169&page=23

[2] The DTIC Review: Human, Social, Cultural and Behavior Modeling (2008). Defense Technical Information

Center, Fort Belvoir VA: Volume 9, Number 1

[3] Gluck and Pew (2005). Modeling human behavior with integrated cognitive architectures: comparison, evaluation, & validation. Lawrence Erlbaum Associates, Inc. Mahwah, New Jersey

[4] Marcel Just, Carnegie Mellon University, 2009 DARPA Workshop on Cognitive Modeling's Limitations

[5] Adolphs, R. (2003). Cognitive neuroscience of human social behavior. Nature Reviews Neuroscience 4, 165-178.

[6] Philiastides, MG, & Sajda, P. (2007) EEG-Informed fMRI Reveals Spatiotemporal Characteristics of Perceptual Decision Making, Journal of Neuroscience . 27(48):13082-91

[7] Linden, DE, & Fallgatter, AJ. (2009). Neuroimaging in psychiatry: from bench to bedside. Frotiers in Human Neuroscience. 3:49.

KEYWORDS: Neuroimaging, cognitive modeling, cognition, thinking, decision making

OSD10-HS4 TITLE: Dynamic Meta-Network Analysis

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: To develop methods and tools to visualize dynamic meta-data social networks and to assist with the analysis of the interdependencies of complex social networks.

DESCRIPTION: Terrorist organizations and other covert groups have network structures that are cellular and distributed, distinct from those in typical hierarchical organizations. Therefore, determining how to attack dynamic networked organizations or how they are likely to evolve, change, and adapt is extremely problematic. Most intelligence sources construct social networks with multiple node classes and multiple different relations between nodes. Research that narrowly focuses on single mode networks does not provide adequate information on interdependent relationships and effects (i.e. being able to distinguish between nodes that are high in information vs. brokers of resources for example is an important capability).

Dynamic meta-network analysis is an emergent scientific field that extends the power of thinking about networks to the realm of large scale, dynamic systems with multiple co-evolving networks involving cognitively realistic agents. With a meta-network perspective, a set of networks connecting various entities such as people, groups, knowledge, resources, events, or tasks are combined to describe and predict system behavior. What is needed is a series of tools and techniques for collecting data on and reasoning about these covert networks even in the face of incomplete or uncertain information.

PHASE I: Analyze the interdependencies in complex social dynamic meta-networks. Provide an approach to building visualization/decision support tools and/or methods to enhance and aid analysis of complex social networks and provide actionable analysis products.

PHASE II: Build demonstration tools and/or methods to quantify improvements over status quo in social network visualization. Develop at least 3 use cases to demonstrate quantifiable improvements in providing visualization capability to analysts. Quantification should include, as a minimum, a reduction in time to produce actionable analysis products.

PHASE III: Build prototype tools and/or methods that can demonstrate real world application improvements. Historical exercises/analysis should be demonstrated clearly showing quantifiable improvements in actionable analysis products.

REFERENCES:

[1] Freeman, Linton C., Visualizing Social Networks, Carnegie Mellon: Journal of Social Structure, V1, 2000

[2] Freeman, L.C, Webster, C.M., and Kirke, D. M., Exploring Social Structure Using Dynamic Three-Dimensional Color Images, Social Networks, 20, 1998, p109-118

[3] Wollman, Matt, Digital Information Graphics, Watson-Guptill Publications, Inc., 2002

[4] Jeffrey Heer and Danah Boyd. Vizster: Visualizing online social networks. In INFOVIS '05: 2005 IEEE Symposium on Information Visualization. IEEE Computer Society, 2005.

[5] Sharabati, W.K., Wegman, E.J. and Said, Y.H. (2009) "Multi-mode social networks", Proceedings of the Human Behavior-Computational Modeling and Interoperability Conference (CD), Oak Ridge, TN: ORNL.

KEYWORDS: Social networks, Dynamic networks, Intelligence, Visualization

OSD10-HS5 TITLE: Visualization Methods and Tools for Human, Social, Cultural, and Behavioral Models

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: To develop visualization and related tools for translating human, social, cultural, and behavioral (HSCB) model outputs to decision-support products.

DESCRIPTION: The intent of HSCB models is to provide decision making support for commanders at all levels for operational planning and effects assessment. The human ability to process visual information can augment analysis, especially when analytic results are presented in iterative and interactive ways. Analysis of HSCB model output introduces significant challenges in data visualization and will require new approaches for representing complex, dynamic data sets. Military leadership would benefit from being able to see and adjust socio-cultural aware Courses of Action (COAs) and impacts, especially in the form of or relative to geo-spatial features. Current model results as expressed in a variety of social-science factors (ethnographic, religious, economic, political, etc) do not adequately support the development of socio-cultural aware Courses of Action (COAs).

Effective visualization tools would enable commanders to:

- collect, validate, visualize, and disseminate data to determine current baselines;
- leverage computational modeling capability to determine trends in an effort to better plan operations in a specific cultural environment;
- develop socio-cultural aware COA designed to support the commander's objectives;
- rank order the COAs as a series of proposed Diplomatic, Information, Military, and Economics (DIME) and Political Military Economic Social Infrastructure Information (PMESII) actions;
- forecast 2nd and 3rd order effects; and
- extract and monitor metrics such that effects can be understood in the relevant operational context.
- develop generalized methods/tools for displaying the uncertainty in dealing with the dynamic complexity of human behavior, beliefs and cultures

Visualizations should provide rich information displayed in appropriate and effective formats (graphics, text, numbers, images, etc) and have the ability to be placed in larger contexts – for instance, geo maps overlaid with economical, sociological and/or historical data. Model visualization may include static images as well as animation and interaction which in some instances may lead to better analysis and enhanced understanding. Visualizations may be designed to take advantage of the largest gigapixel wall-size displays available today , a desk-top workstation, virtual reality systems, or portable electronic devices.

PHASE I: Evaluate and identify visualization methods that provide insight/utility to user community. Identify existing HSCB models for potential integration opportunities. Establish data requirements and perceptual and cognitive processing methods to improve the usability/inference capability from model outputs Provide approach to

visualization tool development and specify expected benefits through the development of measurement of effectiveness.

PHASE II: Build prototype visualization tool that conforms to a specified HSCB model output. Develop at least 3 use cases to demonstrate the enhanced visualization capability of the tool. Use cases should demonstrate improved visualization using dynamically changing qualitative social/cultural data and the use of geo-spatial features.

PHASE III: Integrate visualization tool / methods into specified HSCB model. Demonstrate and validate usefulness of visualization tool through the display of HSCB model output under operational conditions. Tool should demonstrate a greater intuitive situational awareness and decision support, and the ability to provide for deeper understanding of underlying models assumptions/limitations.

REFERENCES:
[1] C. R. Johnson, R. Moorhead, T. Munzner, H. Pfister, P. Rheingans, and T. S. Yoo, (Eds.): NIH-NSF Visualization Research Challenges Report; IEEE Press, ISBN 0-7695-2733-7, 2006.

[2] Edward R. Tufte, The Visual Display of Quantitative Information, Graphics Press, Seventeenth Printing, April 1999

[3] Andries van Dam, David H. Laidlaw and Rosemary Michelle Simpson, Experiments in Immersive Virtual Reality for Scientific Visualization, Computers & Graphics, Volume 26, Issue 4, August 2002, Pages 535-555

KEYWORDS: Information Representation, Visualization, Geovisualization, Virtual Reality

OSD10-HS6 TITLE: Automated Network Construction

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: The objective of this topic is to develop tools to automate/speed the construction of dynamic meta-data social networks to aid analysis of the interdependencies of complex social networks.

DESCRIPTION: The most time consuming part of network analysis is network construction. Tools that help the analyst determine network relationships through automation and/or through "wizard" help/dialog systems may help reduce construction time and allow for more detailed actionable intelligence and/or faster delivery to supported units. Existing tools (e.g. Organizational Risk Analyzer (ORA)) are based on social science theories and have import and visualization tools. However, as general purpose tools, these network analysis products require significant training and human-in-the-loop interaction to produce useable analysis products. Tools should be designed to work with these products (vice building a new standalone product) to provide improved performance in development of analysis products.

PHASE I: Analyze the bottlenecks/challenges to rapid construction of dynamic meta-data social networks. Provide approach to development of tools/methods to reduce the time to construct social networks. Approach should quantify expected gains through tools/methods.

PHASE II: Build demonstration tools/methods that show quantifiable improvements over status quo in complex social network constructions. Develop at least 3 use cases to measure improvements in constructing networks and resultant analysis products. Quantification should include, as a minimum, a 50% reduction in time to produce actionable analysis products.

PHASE III: Build prototype tools/methods that can demonstrate real world application improvements. Historical exercises/analysis should be used to clearly demonstrate quantifiable improvements in network construction and actionable analysis products.

REFERENCES:

[1] Carley, Kathleen & Reminga, Jeffrey & Storrick, Jon & DeReno, Matt. (2009). ORA User's Guide 2009. Carnegie Mellon University, School of Computer Science, Institute for Software Research, Technical Report CMU-ISR-09-115

[2] Carrington, Peter J. & Scott, John & Wasserman (editors), Stanley, Models And Methods In Social Network Analysis, Cambridge ; New York : Cambridge University Press, 2005

[3] Wasserman, Stanley, and Faust, Katherine, Social Network Analysis: Methods and Applications. Cambridge: Cambridge University Press. 1994

KEYWORDS: Social networks, Dynamic networks, Intelligence, Social network analysis

OSD10-HS7 TITLE: Analytical Tools for Local Economic Analysis

TECHNOLOGY AREAS: Information Systems, Human Systems

ANALYTICAL TOOLS FOR LOCAL ECONOMIC ANALYSIS

OBJECTIVE: Provide an analytical tool that will enable Marines/Soldiers at the company or lower level to assess local economic conditions and develop courses of action to impact the economy.

DESCRIPTION: Stability and Counterinsurgency operations require Marines and Soldiers to adapt and influence rapidly changing conditions and perform many nonmilitary tasks. Included in these nonmilitary tasks is economic stabilization and development. Sound economic stabilization policies create conditions for economic growth, which alleviates underlying tensions and addresses the chronic social conditions that can fuel insurgency or conflict. In order to understand and influence the changing local economic situation, Marines and Soldiers need tools that allow them to collect and analyze local economic data from both formal and informal (black) markets in order to inform their courses of action as they relate to supporting local economic development. Data required for these analyses must be easily accessible. These tools must be usable with little or no training (less than 2 hours) by non-experts (high school education).

PHASE I: Identify key elements of a local economy that are relevant to the company or lower level marines/soldiers and identify appropriate methods for analyzing local economics. Provide approach for developing an analytical tool for assessment of local economic conditions. Provide methodology to effectively and rapidly train marines/soldiers on the use of such an analytical tool and on how local economic conditions may affect broader stabilization and development objectives.

PHASE 2: Design and build prototype analytical tool including training curriculum.

PHASE 3: Develop and integrate analytical tool with hardware that meets requirements of deployed warfighter (portable, hardened, etc.).

REFERENCES:

1. Keith Crane, Olga Oliker, Nora Bensahel, Derek Eaton, S. Jamie Gayton, Brooke Stearns Lawson, Jeffrey Martini, John L. Nasir, Sandra Reyna, Michelle Parker, Jerry M. Sollinger, Kayla M. Williams; Guidebook for Supporting Economic Development in Stability Operations, RAND Corporation, Santa Monica,CA, ISBN 978-0-8330-4634-5.

2. Joint Publication (JP) 3-57, Civil-Military Operations, July 2008.

3. Field Manual 3-07 Stability Operations, Department of the Army, October 2008

KEYWORDS: Stability Operations; Counterinsurgency; Economic Analysis; Analytical Tools

OSD10-HS8 TITLE: An Adaptive Cultural Trainer for Development of Cultural Aptitude in Warfighters

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: The objective of this topic is to develop an adaptive virtual environment (VE) that adjust to level difficulty in response to neurophysiological metrics and that incorporates adaptive cultural models to show how interactions with local populations affect shifts in local opinion, perception, movement, and so forth

DESCRIPTION: The U.S. military is currently undergoing more and more non-kinetic operations overseas and needs a better understanding of how cultural interactions with individuals and/or leaders in a community can affect the local population. As Irregular Warfare (IR) becomes of greater importance to the military, the training tools for cultural settings must increase and adapt as well. How warfighters interact with local population affects the population's movements, perceptions, opinions, and so forth. VE simulations that allow warfighters to practice both language and cultural skills could benefit from incorporating social network, cultural, and geospatial models in order to show how interactions with local populations affect societal changes and shifts in local opinion, perception, movement, and so forth.

Currently, language/cultural trainers teach language and cultural skills without population scenarios and first person shooter trainers do little to teach language or cultural skills. For example, if a player makes a poor decision say by insisting on speaking directly to a young single female when her older uncle is there, instead of speaking through her uncle to her, the program does not model how that interaction affects the local population's opinion, perception, movement, and so forth. By creating simulations where warfighters can learn cultural negotiation skills, cultural aptitude, and language a new cultural trainer that incorporates all the behaviors and types of interactions a warfighter will be called on to perform, as well as incorporating adaptive models, warfighters will be better able to see how their actions and reactions to events impact not only the person they are interacting with but the population as a whole.

The proposed solution will leverage an existing cultural and language trainer and incorporate social network, cultural, and geospatial models effects on population parameters. Trainees will be able to speak to and interact at any level with indigenous non-player characters (NPC), complete with voice recognition, speech, and facial gestures. The characters will react according to how the trainee interacts with them. Further the game will track how the local population reacts to these interactions. The game will adapt to changes in local population response. For example, if a player comes in and insults the local tribal leader the game scenario will change and the trainee will find that future interactions with the local population are more difficult and more hostile. In addition, the trainee will be monitored for neural/physiological markers (e.g. EEG, eye tracking, pupil diameter, heart rate, respiration, and so forth) of workload and the game will adjust in difficulty based in part on these neural/physiological metrics; this is designed to keep players motivated, interested, and at an optimal learning level. To assess users' performance, trainees' behavioral responses in the game will also be monitored.

PHASE I:
1. Develop a culture-general framework that links into the backend of an existing language and culture trainer. The program being developed should be able to implement culture-specific models that gauge interactions between gamers and NPC and model how the virtual population adapts their views of the individual (i.e. gamer), the U.S. military, coalition forces, and so forth.
2. Develop goal-oriented scenarios for warfighters of different levels (e.g. commanders might be talking to regional leaders, while lower enlisted men would only be talking to civilians) and for different segments of the target population (e.g. Sunnis vs. Kurds and so forth).
3. The program will need to be able to support interactive training from one to four players (i.e. individual to fire team).

PHASE II:
1. Develop a prototype system based on the preliminary design from Phase I. An After Action Review module will show users how their interactions with the NPC affected not only the NPC but the population as a whole. Allow for

repeated interactions where prior conversations are used to shape attitudes coming into new scenarios.
2. Incorporate neurophysiological metrics (i.e. using EEG and eye tracking) in order to gauge workload in the trainees. Create adaptive scenarios that use neurophysiological metrics to keep trainees in an optimal state of learning.

PHASE III:
1. This technology will have broad application across military, governmental organizations, and non-governmental organizations; as well as in commercial settings.
2. This technology will expand on the militaries current ability to train warfighter's cultural aptitude.

REFERENCES:
[1] Deaton, J.E., Barba, C., Santarelli, T., et al. (2005). Virtual environment cultural training for operational readiness (VECTOR). Virtual Reality, 8, 156–167.

[2] Berka C, Levendowski DJ, Lumicao MN, et al. (2007). EEG correlates of task engagement and mental workload in vigilance, learning, and memory tasks. Aviat Space Environ Med, 78(5, Suppl.), B231-B244.

[3] Wierwille, WW, Rahimi, M, Casali, JG, (1985). Evaluation of 16 Measures of Mental Workload using a Simulated Flight Task Emphasizing Mediational Activity. Human Factors: The Journal of the Human Factors and Ergonomics Society, 27(5), 489-502.

KEYWORDS: Training; Cultural Aptitude; Virtual Environments; Adaptive Training; Workload; Social Networks

OSD10-HS9 TITLE: Developing and Modeling Social Networks inside Technology Poor Societies

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: The objective of this topic is to develop tools that enable the legitimate local civil authority to establish open lines of communication with the local population and to develop a technology platform that leverages this communication system allowing the armed forces to identify and monitor social networks within the local population in real-time.

DESCRIPTION: Traditional combat doctrine recognizes five phases of warfare – from Phase 0 (Shaping and influencing the state of affairs in peacetime) through Phase 4 (Stabilizing). Successful conduct of traditional warfare required an intimate knowledge of the physical terrain. With this knowledge weaker forces have been able to conquer superior forces, outmaneuver larger forces, and prolong battles until reinforcements were able to arrive. In irregular warfare, however, the human terrain becomes much more important as it is constantly shifting, moving, and being informed by many variables in within and between local populations. Irregular and non-kinetic warfare also adds a sixth phase to the traditional combat doctrine (Enabling Civil Authority). This phase represents the beginning stage of enabling local government to ultimately gain the authority it needs to function. An important component in establishing local government authority is the establishment of effective bidirectional lines of communication between the governors and the governed. In many areas of the world the idea of bidirectional communication is very novel and requires not only the tools necessary for communication but methods to gain acceptance with those involved and ways by which the local population can be monitored. Local populations can be divided into friends, enemies, and a gray population who is neither friend nor foe. In irregular warfare we need to monitor changes within these three populations with regards to their attitudes and behaviors toward us (i.e. are we winning hearts and minds) and the established governing authority (i.e. is the local government being accepted by the population). Successful conduct of irregular warfare requires that commanders have up-to-date knowledge of this human terrain. Models and techniques need to be developed that accurately measure changes in the gray population.

Today we are very good at modeling this type of human terrain in "technology rich" populations. We have models of human social networks that can inform us about societal changes and shifts in local opinion, perception, movement, and so forth. We have developed good techniques for acquiring this data. The problem is that these

methodologies rely on technology (i.e. mobile phone data, the internet, and so forth). In "technology poor" societies the technology infrastructure is not as developed making this type of data collection difficult or impossible. Further, this lack of technology infrastructure also leads to break down in bidirectional communication. In these situations bidirectional communication is often established through the presence of military advisors (i.e. leaders who attempt to transfer first-world notions of government to what are often third-world governments). Due to cultural differences and the impression of one-way directives imputed on the emerging civil authority these efforts are not always effective.

A more effective solution would be to provide the emerging civil authority with tools through which they could establish their own communication protocols. These tools would first supplement and reinforce the training and experience they receive while working with military advisors. Subsequently, they would form the basis of communication between the people and their newly established civil authority. Further, these technologies should be easy to use by populations with various levels of education and technical expertise. Any solution modeling human terrain would capitalize on these communication protocols to identify and monitor social networks in real-time. This proposed solution will give the armed forces the ability to predict, prevent, outmaneuver, and rapidly respond to unfavorable changes and trends in local population.

PHASE I: 1. Develop a cultural-general situation independent framework for establishing communication protocols in various emergent threat situations. These protocols should be flexible enough to be useable in any kinetic or non-kinetic scenario. In addition, these protocols should be general enough that any emerging civil authority can modify them to their own situations.
2. Develop a technology adoption/transition strategy for the communication protocols.
3. Develop a technology platform that can be used to assess the current state of technology use in a given society (i.e. mobile phones, computers, internet, television radio, and so forth). The platform needs to be able to project how quickly technology is being adopted.
4. Identify current technology that could be used in these scenarios to allow rapid implementation of the communication systems.
5. Develop a technology platform that leverages these communication protocole enabling social networks to be identified and tracked in real time.

PHASE II: 1. Develop, demonstrate, and validate a prototype system based on the preliminary design from Phase I.
2. Demonstrate the effectiveness of a deployed prototype in an operational setting. Deployed prototype should be able to withstand operational use for a period of no less than 12 months without significant failure or interruptions during field testing. Significant failure or interruption of the communication system shall be defined as a failure due to design or engineering (not acts of God and/or War) standards.
3. Demonstrate the ability of the prototype system to monitor social networks and make accurate predictions of behavioral changes, movements, and trends in the population in real-time.
4. Develop training standards of military advisors in the use and implementation of the protocols and communication systems within emerging civil authority.

PHASE III: 1.This technology will have broad implication for military and humanitarian situations where communication between the government and the local population has been disrupted and/or destroyed and needs to be reestablished.
2. This technology will have broad application in military intelligence, as well as provide policy makers with valid societal information and predictive trends. Further, this technology has broad applications in commercial settings helping companies understand the human terrain prior to entering emerging markets.

REFERENCES:
[1] Berteau, D, Brannen, SJ, Douglas, E, Freier N, Murdock, CA, Wormuth, CE. (2008). Transitioning Defense Organizational Initiatives. An assessment of key 2001-2008 defense reforms. Available at: http://www.stormingmedia.us/14/1441/A144194.html

[2] NATO Parliamentary Assembly (2004). Military involvement in civilian and humanitarian missions. Montreux, Switzerland. March 2-4, International Secretariat report

[3] Crowley, J, Currion, P, Frost, E, Graham, J, Griffiths, P, Hanchard, D, et al., (2006). Stability, Security,

Transition, and Reconstruction: Observations and Recommendations from the Field. Version 20061103:1.1; The Strong Angel Team. Available at: http://mindtel.com/2007/0508.ops-memes/Strong%20Angel%20Recommendations%20in%20SSTR.pdf

[4] Eagle, N., Pentland, A., & Lazer, D., (2009). Inferring Social Network Structure using Mobile Phone Data. Proceedings of the National Academy of Sciences, 106(36), 15274-15278.

[5] Eagle, N. & Pentland, A., (2009). Eigenbehaviors: Identifying Structure in Routine. Behavioral Ecology and Sociobiology, 63(7), 1057-1066.

[6] Raento, M., Oulasvirta, A., & Eagle N., (2009). Smartphones: An Emerging Tool for Social Scientists. Sociological Methods Research, 37(3), 426-454.

[7] Tong H., et al. (2008). Fast mining of complex time-stamped events. 17th ACM conference on Information and knowledge management, 759-768.

KEYWORDS: Social Networks; Data Mining; Human Terrain; Real-Time Behavioral Monitoring, Civil Authority, Social, Cultural, Transition, Reconstruction, Civilian

OSD10-IA1 TITLE: Countermeasures to Malicious Hardware to Improve Software Protection Systems

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop innovative countermeasures to malicious hardware modifications for the purposes of developing trusted software protection systems.

DESCRIPTION: Software protection system design methodology has focused on reducing the vulnerabilities of those systems to attack by reducing the dependence on untrusted components and making critical information inaccessible to the adversary [1]. These protection systems run primarily on commercial-off-the-shelf (COTS) computers, but often rely on tamper-proof hardware built using COTS parts to provide a secure mechanism to store critical data and/or execute critical pieces of the application being protected [2]. However, the security of the protection system depends on the trustworthiness of the underlying hardware components that are running and storing the software and data. These components include the parts on COTS computer systems on which the applications execute (or partially execute) as well as the COTS parts from which custom hardware-assisted protection solutions are built [2].

National security concerns have been raised over the outsourcing of chip fabrication and other integrated circuit manufacturing overseas, since these devices are used in DoD weapon systems. The risk is that if an adversary can maliciously alter hardware and/or firmware on printed circuit boards, integrated circuits, or reconfigurable components used in DoD systems, the device functionality can be altered, privileges escalated, critical data leaked, or denial-of-service attacks levied on the system at a later date and time when those systems are operational [3]. To add to the risk, hardware can be altered at other stages in the systems engineering process, including design, manufacturing, packaging, integration, and deployment, through the use of third party software/firmware tools used to program the devices or via direct hardware modifications, even within the United States.

The goal of this research is to design and develop non-destructive techniques that detect and respond to malicious hardware/firmware modifications that are made for the purposes of software piracy/data exfiltration, reverse engineering, and malicious alteration of critical software applications and data running on COTS systems or whose security system utilizes COTS parts [2]. Solutions of interest include developing countermeasures to hardware Trojans introduced in COTS computer hardware elements (e.g., CPU, chipsets, motherboards, hard disk drives, peripheral cards) [4], as well as attached custom hardware boards or components (such as an FPGA or ASIC) [5] that might be used as part of a hardware-assisted software protection system [2].

Malicious hardware to be considered includes 'functional' Trojans that add malicious circuitry to hardware components [6], 'parametric' Trojans that modify (but do not add to) the original circuitry [7], and firmware Trojans that alter the hardware device functionality [8]. Hardware/firmware Trojan triggering mechanisms to be addressed include internally and externally activated signals, such as (1) rare input data values, (2) time triggering, (3) internal logic state, and (4) external sensors.

Factors to consider in countermeasure development [9] [10] include, but are not limited to, (1) invasiveness of the approach, (2) false positive and false negative rates, (3) types of Trojans detected, (4) ability to detect small Trojans, (5) performance of the detection procedure and the impact on the protected application, and (6) cost.

PHASE I: 1) Develop a concept to detect and respond to malicious hardware/firmware modifications to COTS parts and systems. 2) Research the advantages and disadvantages of the approach (considering the factors stated above). 3) Produce a detailed research report outlining the design and architecture of the system, as well as the advantages and disadvantages of the proposed approach.

PHASE II: 1) Based on the results from Phase I, design and implement a fully functioning prototype solution. 2) Emulate a hardware Trojan on a COTS part and demonstrate its effectiveness in compromising a software protection system. 3) Provide test and evaluation results that demonstrate the effectiveness of the solution to detect and react to the hardware Trojan demonstrated in 2). 4) Develop a final report enumerating the specific threats addressed and countermeasures developed in the prototype solution.

PHASE III DUAL-USE APPLICATIONS: The technology developed under this research topic will mitigate the risk of malicious hardware and improve the trustworthiness of software protection systems. DoD applications that will benefit from this technology include a wide range of embedded systems, such as weapons systems, avionics, communications, and sensor systems. Commercial applications include financial systems, voting machines, communication systems, and SCADA systems. As a result, this technology is vital for both the DoD and commercial organizations.

REFERENCES:

[1] Software Protection Initiative, The Three Tenets of Cyber Security, http://spi.dod.mil/tenets.htm

[2] IBM 476 PCI-X Cryptographic Coprocessor, http://www-03.ibm.com/security/cryptocards/pcixcc/overhardware.shtml

[3] Fouad Kiamilev, et. al., "Demonstration of Hardware Trojans," CVORG, University of Delaware, http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-kiamilev.pdf

[4] Loic DuFlot, "CPU bugs, CPU backdoors and consequences on security," Journal in Computer Virology, Vol. 5, No. 2, May 2009, 91-104.

[5] Ilija Hadzic, Sanjay Udani and Jonathan M. Smith, "FPGA Viruses," http://www.cis.upenn.edu/~jms/papers/fpgavirus.pdf

[6] Francis Wolff, Chris Papachristou, Swarup Bhunia, Rajat S. Chakraborty, "Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme," Case Western Reserve University, http://www.date-conference.com/archive/conference/proceedings/PAPERS/2008/DATE08/PDFFILES/IP5_2.PDF

[7] Y. Shiyanovskii, F. Wolff, C. Papachristou, D. Weyer, and W. Clay, "Hardware Trojan by Hot Carrier Injection," http://arxiv.org/PS_cache/arxiv/pdf/0906/0906.3832v1.pdf

[8] Samuel T. King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou, "Designing and implementing malicious hardware," http://www.cs.uiuc.edu/homes/kingst/Research_files/king08.pdf

[9] Benjamin Sanno, "Detecting Hardware Trojans," Ruhr-University Bochum, Germany, http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/seminare/itsss09/benjamin_sanno.semembsec_termpaper_20090723_final.pdf

[10] Markus Kuhn, “Trojan Hardware – some strategies and defenses,” University of Cambridge, http://www.cl.cam.ac.uk/~mgk25/dagstuhl08-hwtrojan.pdf

KEYWORDS: Malicious Hardware, Hardware Trojans, Firmware Trojans, FPGA viruses, Software Protection, Hardware Supply Chain

OSD10-IA2 TITLE: Effective portable data content inspection and sanitization

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Advance the security, effectiveness, and automation of the malicious code and information leakage detection process for physical media entering or leaving classified or controlled facilities.

DESCRIPTION: Daily operations within DoD research laboratories requires particular care to be taken when introducing new software packages or data into a controlled environment. Typically media entering or leaving a research facility is expected to be scanned for viruses and other malicious content as well as be properly inventoried for reference and control purposes. This process does not take into account inspection for data leakage, deep file inspection for malware, or the potential exploitation of the scanning host by malicious code on the target media. Although there are network based guards which have developed processes to safely perform analysis of files traversing security domains, not all organizations or facilities have access to these devices. Additionally, analysis techniques used by existing network guard solutions for static lists of file types, formats, and expected ranges of data cannot be employed in a research environment where file types, format, and data are as dynamic as the research at hand. Advanced techniques are being employed by adversaries to avoid malware detection using traditional software including obfuscation, packing, and multi-tiered encoding techniques. These key factors are driving the need for the ability to perform a more in depth file analysis for malicious code and data leakage. The focus of this effort is to develop foolproof ways to securely and verifiably identify multiple file types. This can be accomplished via magic numbers, format validation, or other means that can be fully automated. The number of file types this solution addresses should be larger than those currently organized and recognized within the cross domain community. Additional capabilities to check these file types for hidden content automatically and with a high level of assurance would be exceedingly useful. Those file formats which aren’t identifiable by these methods will be put into a quarantine for future additional assessment in either a “detonation chamber” capability or other means. These mechanisms will be expected to operate in controlled and potentially classified environments processing autonomously with no access to external resources, administrative control channels, or a human in the loop review process. The system must be capable of enforcing positive control when a situation or data type is presented that cannot be autonomously managed.

PHASE I: 1) Investigate and propose a mechanism capable of autonomously performing deep file inspection, format validation and verification, virus scanning, malware detection, and quarenteen unknown data types for future analysis.
2) Provide a minimal software prototype demonstrating the feasibility of the concept, to include capabilities currently recognized in the cross domain community as part of current best practices and novel capabilities that extend beyond those best practices.

PHASE II: 1) Based on the results from Phase 1, refine and extend the prototype system to a fully functioning inspection system with additional inspection capabilities for quarantined data.
2) Provide an analysis demonstrating significant improvement in detection of malicious code and hidden data.
3) Provide an analysis demonstrating the robustness of the system to withstand an attack via malicious code.
4) Provide measurements of each step within the system to include performance metrics. These measurements will be expected to be useful for situational awareness.

PHASE III: Government and commercial entities are required to ensure absolute security of research facilities from malicious code and data leakage. Therefore, an effective, secure means to provide controlled inbound and outbound data inspection would be marketable to governmental and commercial entities.

KEYWORDS: malicious code, data leakage, malware detection, deep file inspection, malicious content inspection , hidden data detection

OSD10-IA3 TITLE: Robust and Efficient Anti-Phishing Techniques

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Development of high-accuracy, low-latency automatic identification and mitigation techniques to detect and stop phishing attacks.

DESCRIPTION: Phishing has evolved from a nuisance into a top security concern. As the number, cost, and complexity of phishing attacks continue to increase, robust and effective techniques are critically needed to counter the new threats. Existing solutions such as spam filters rely heavily on manually maintained blacklists of phishing websites, and are not robust at catching phishing emails, especially spear-phishing attacks, since these attacks look just like legitimate emails. By their very nature, manually maintained blacklists are always lagging one step behind. The general task of identifying phishing emails and URLs is challenging for several reasons. The most significant of these are: (i) attacks are designed to look legitimate (e.g. traditional bag of words methods used in many spam filters don't work and the same is true for phishing URLs); (ii) phishing kits have become more sophisticated, enabling phishers to quickly launch attacks that involve constantly changing URLs ("fast flux attacks"); (iii) some targeted attacks are sent to a very small number of people and leverage information that is unique to a given organization (e.g. names of employees, seemingly legitimate email addresses, etc.); (iv) people lack the necessary sophistication and training to detect many of these attacks, thereby requiring the help of automated solutions to fend them off; (v) hybrid attacks make detection increasingly difficult and can be designed to explore a wide variety of vulnerabilities (e.g. DNS poisoning, bots, infected websites); (vi) solutions need to be designed to have extremely low (near-zero) false positive rates, otherwise users are forced to manually review decisions made by filters, which defeats the whole purpose of deploying these filters in the first place. To meet these challenges, more sophisticated, multi-faceted approaches need to be developed to catch a higher percentage of phishing attacks (e.g. phishing emails and phishing URLs) with a near-zero false positive rate. The desired solutions need to rapidly identify suspicious emails with a high confidence and can selectively escalate analysis when needed.

PHASE I: 1) Research and develop novel heuristic-based, adaptive, and intelligent solutions that can accurately identify phishing attacks (catching a high percentage of attacks) while keeping false positive rates near zero and with a low latency; 2) Demonstrate that the proposed techniques can scale to high traffic volumes and are capable of addressing a wide range of phishing attacks (e.g. emails with and without links in them)

PHASE II: 1) Develop a working system to demonstrate its effectiveness against various types of phishing attacks on live traffic; 2) Carry out benchmarking experiments with synthetic traffic generators and information feeds representative of actual traffic flows. Validate system effectiveness under real operational testing.

PHASE III -- DUAL-USE COMMERCIALIZATION: Effective phishing attack mitigation is a critical capability for both the military and commercial sectors. The developed technology will be useable on both government networks and commercial networks. The developed system should be marketed as a product that can easily be deployed alongside existing legacy filters.

REFERENCES:
1. I. Fette, N. Sadeh, and A. Tomasic, Learning to Detect Phishing Emails In Proceedings of the 16th International Conference on World Wide Web, Banff, Alberta, Canada, May 8-12, 2007.

2. S. Abu-Nimeh, D. Nappa, X Wang, S. Nair, A comparison of machine learning techniques for phishing detection Proceedings of the anti-phishing working groups.

3. G. L'Huillier, R. Weber, N. Figueroa, Online phishing classification using adversarial data mining and signaling games, Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics.

4. J. Wang, R. Chen, T. Herath, H. R. Rao, 2009. "An Exploration of the Design Features of Phishing Attacks." In Annals of Emerging Research in IA, Security and Privacy Services, edited by H.R. Rao and Shambhu Upadhyaya. Emerald.

5. Y. Zhang, J. Hong, and L. Cranor, CANTINA: A content-based approach to detecting phishing web sites. In Proceedings of the 16th International conference on World Wide Web, Banff, Alberta, Canada, May 8-12, 2007.

OSD10-IA4 TITLE: Preventing Sensitive Information and Malicious Traffic from Leaving Computers

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Research and development of real-time, automatic identification and mitigation techniques to detect and stop unauthorized information leaking as well as unwanted and malicious traffic emanating from a computer at all time and locations. New techniques and implementations are needed to monitor applications and user activities on a computer to detect and stop outgoing data and traffic that is not intended or authorized by the user or security policies.

DESCRIPTION: Malicious software on compromised computers, e.g., spyware, botnets, Remote Administration Trojans, key loggers, peer-to-peer file sharing, remote monitoring and control software constitute serious threats to DoD systems because they run inside DoD networks collecting information, and then surreptitiously send information out. Network security appliances (such as a network intrusion detection system) that focus on traffic analysis provide limited help to detect and stop information leaking and malicious traffic from compromised computers. Distinguishing human- vs. malware- generated data from a network traffic analysis perspective is extremely challenging. Current anti-spyware and anti-virus systems have a large capability gap in finding and stopping spyware and other malicious software running on computers, especially when malware can get into the operating system kernel and disable these on-host security systems. Robust, accurate, and efficient monitoring of applications and user activities on a computer, particularly actions that relate to outgoing data and traffic, is a promising approach to ensure that data and traffic leaving a computer is indeed authorized by security policies. The general task of identifying and stopping unintended and unauthorized traffic is challenging for several reasons. First, for the monitoring system to be effective and practical, it must be robust and efficient, cannot be disabled by malware, and with no/low noticeable performance overhead. Second, current virtual machine technologies are "heavyweight" thus a light weight approach is desired. Third, precisely identifying applications and user events related to outgoing data and traffic and ensuring that the observations are not forgeable require accurate understanding of application semantics, memory analysis, and handling of hardware events in a very efficient manner. To address these challenges, new architecture that can combine the benefits of both out-of-VM and in-VM monitoring approaches, systems that comes with lightweight, transparent hypervisor, and techniques that can precisely and securely identify user actions and application activities and data are highly desired. This will mitigate common problems that current techniques have: the monitoring system could be disabled by malware, user events or data could be forged by malware, or monitoring is too slow for the system to be practical.

PHASE I: 1) Research and develop an architecture that can combine the benefits of both out-of-VM and in-VM monitoring approaches and new techniques for accurate and efficient understanding of application semantics, memory analysis, and handling of hardware events. 2) Demonstrate the proposed architecture and techniques with a typical computer (e.g., Intel/AMD hardware) and software configurations (e.g., commodity operating systems and applications).

PHASE II: 1) Develop a working system that can in real-time automatically stop unintended or unauthorized outgoing data and traffic, while producing no false alarms, when tested live with a user/computer. 2) Carry out comprehensive benchmarking experiments using representative usage scenarios of varying application programs and malicious software and demonstrate the advantages of this approach by comparing against existing tools and techniques.

PHASE III/DUAL USE COMMERCIALIZATION: Effective (host) computer security, in particular, information leaking mitigation is a critical capability for both the military and commercial sectors. The developed technology

will secure both military and civilian computers. The new monitoring system should be marketed as a standalone product or can be licensed to a third party.

REFERENCE:
1. W. Cui, R. H. Katz, and W. tian Tan. Design and Implementation of an Extrusion-based Break-In Detector for Personal Computers. In Proceedings of the Annual Computer Security Applications Conference (ACSAC), 2005.

2. R. Gummadi, H. Balakrishnan, P. Maniatis, and S. Ratnasamy. Not-a-Bot (NAB): Improving Service Availability in the Face of Botnet Attacks. In Proceedings of the USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2009.

3. Monirul Sharif, Wenke Lee, Weidong Cui, and Andrea Lanzi. Secure In-VM Monitoring Using Hardware Virtualization. In Proceedings of The 16th ACM Conference on Computer and Communications Security (CCS 2009), Chicago, IL, November, 2009.

KEYWORDS: Secure OS, data exfiltration prevention, virtual machine monitoring,

OSD10-IA5 TITLE: Biometric-based Computer Authentication during Mission Oriented Protective Posture Scenarios

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop a biometric-based approach to automatically authenticate a user, encumbered in full Military Oriented Protective Posture (MOPP) Level IV gear, to a network/host.

DESCRIPTION: MOPP gear is full-protection chemical protective gear for warfighters. This gear consists of a carbon-filter suit, chemical protective mask, and rubber gloves and boots. This technology provides a warfighter, in full protective MOPP gear, to walk up to a networked computer host and be automatically biometrically authenticated into the machine, without having to use a Common Access Card (CAC) card or type in a username/password.

In the height of battle, warfighters on the ground at forward operating bases will likely need to wear MOPP gear to protect against chemical and biological threats, while executing their critical war fighting duties using computer networks. MOPP Level 4 is the most protective, but the most encumbered and inhibiting to the warfighter's movement, visual horizon, and finger dexterity.

It is important that the authentication be strong 3-factor authentication, utilizing single or multimodal biometrics. The system must provide provable, non-repudiable identity of 100% of individuals uniquely, 100% of the time. It is envisioned that any special device worn by the warfighter be small, portable, and non-intrusive (such as a bracelet, ID-tag, "dog tag", etc.). The device would likely need to transmit the authentication information securely and wirelessly (in an RFID-like fashion for example) over a short range (3-5 feet). The device should provide continuous authentication with the human while it is being worn, such that the wearer should not need to regularly re-authenticate to the device. The security implementation must be simplified for the warfighter to use.

PHASE I: Conduct a feasibility study on the design and development of a technology that incorporates 3-factor authentication, capable of uniquely identifying a user via biometrical methods, that could be used during full Military Oriented Protective Posture (MOPP) Level IV gear operations. The biometrical identification method must be able to uniquely identify a person to a high level of fidelity and allow incorporation into a working prototype during phase II.

PHASE II: Develop a working prototype and utility model that allows a user to automatically authenticate a user, encumbered in full Military Oriented Protective Posture (MOPP) Level IV gear, to a network/host.

PHASE III: Extend or logically conclude this SBIR effort performed under prior program phases or funding.

Technology could be expanded across all work environments within DoD, to include normal office environments, engineering rooms, flight lines, and clean rooms. Additionally, the technology could provide authentication for physical space/building access, weapon system control consoles, and secure container and records access. Civilian applications include provable identity for medical, financial, and commerce transactions, such as automated authentication at ATMs, grocery stores, banks, and hospitals.

REFERENCES:
1. http://en.wikipedia.org/wiki/MOPP

2. http://en.wikipedia.org/wiki/Biometrics

3. http://en.wikipedia.org/wiki/Multi-factor_authentication

KEYWORDS: multi-factor, continuous, authentication, biometrics, information security, cyber, computer, security, computer defense, network access, wireless, RFID

OSD10-L01 TITLE: Temporal and Conceptual Extractions of Complex Social Network Data

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop a knowledge extraction technique suitable for large datasets of fused multi-source sensor information that can identify and predict adaptations in a terrorist network. Provide a capability for tactical decision makers to understand shifts in terrorist organizations, such as new sources for recruiting members, new concepts for terrorist activities, and temporal elements of terrorist behaviors.

DESCRIPTION: A software prototype for discovering and displaying visually temporal and conceptual elements of a social network (that could be extended to a terrorist network).

Social network analysis is a valuable methodology for understanding relationships of social groups [1], tracing interactions among individuals [2], and describing data diffusion behavior in delay tolerant networks [3]. The growth of information available from on-line social networking sites and the availability of multi-source sensors has produced a corpus of data that, if sufficient data mining capabilities existed, could aid intelligence analysts in understanding terrorist intentions in near-real time [4]. For such a capability to be realized several developments are required.

The first is a focus on communication technologies favored by the social group of interest. Given interest in social groups that may be relatively unknown, such as terrorist groups or emergent social groups [e.g., followers of new trends], a method to deal with and model uncertainty in the context of past behavior may be of potential use [4]. The second is the ability to extract components of social influence in large-scale networks [5]. The knowledge seeker also must identify and track new influences and must be able to determine the spread and strength of followers' commitment. The third requirement is metrics that define temporal distance in the behavior of the social network. Examples of temporal distance could include frequency of contacts between nodes or groups, inter-contact time, recurrent contacts, time order of contacts along a path, and delay path of information spreading processes [6]. It quickly becomes clear that adding temporal aspects of group behavior in a social network can become difficult to view and, therefore, analyze. Novel visualization techniques will be necessary in order for analysts to extract knowledge, such as those identified in [7]. Perhaps the most difficult but most important requirement for the future of social network analysis is the ability to identify emergent concepts and to link those with observed network behaviors or associations. To the extent that knowledge extraction techniques can identify human conceptualizations, such as the techniques identified in [8], the needle in the haystack may become less elusive.

Challenges for this topic include 1) identifying new social network associations that include communication technologies as an identifiable factor, 2) developing methods to extract features associated with social influence in groups, 3) defining and testing metrics for describing temporal aspects of social network behavior, and 4) identifying methods to predict novel concepts that arise from social behavior and attitudes.

Several large unclassified datasets will be made available to the contractor to develop these prototype software services, algorithms, and social network metrics. Alternately, the contractor could use open source data sources. The OSD is interested in innovative R&D that involves technical risk. Proposed work should have technical and scientific merit. Creative solutions are encouraged.

PHASE I: Complete a literature review, feasibility study and research plan that establishes the proof of principle of the approach for analyzing large datasets with a text/biometric software extraction tool capable of producing social network metrics that utilize temporal and conceptual aspects. Identify the critical technology issues that must be overcome to achieve success. Prepare a revised research plan for Phase 2 that addresses critical issues.

PHASE II: Produce a prototype system that is capable of producing meaningful social network graphs from a corpus of uncertain data that can provide meaningful prediction of human behavior in relation to temporal and conceptual aspects. The prototype should lead to a demonstration of the capability. Test the prototype in an environment to demonstrate feasibility. Demonstrate a capability to construct social network graphs using novel algorithms that support conceputal knowledge discovery in dynamic time periods.

PHASE III: Produce a system capable of deployment in an operational setting of interest. Test the system in an operational setting in a stand-alone mode or as a component of larger system. The work should focus on capability required to achieve transition to program of record of one or more of the military Services. The system should provide metrics for performance assessment.

REFERENCES:

1. Waskiewicz, T. & LaMonica, P. (2008). Developing an intelligence analysis process through social network analysis. In M. Blowers and Alex F. Sisti, Eds., Evolutionary and Bio-Inspired Computation: Theory and Applications II, Proceedings of SPIE Vol. 6964, 69640B.

2. Kahn, M. U. & Khan, S. A. (2009). Social networks identification and analysis using call detail records. ACM: ICIS, November 24-26, Seoul, Korea.

3. Zhang, Y. & Zhao, J. (2009). Social network analysis on data diffusion in delay tolerant networks. ACM: Proceedings of MobiHoc 09, May 18-21, New Orleans, LA.

4. Drozdova, K. & Samoilov, M. (2009). Predictive analysis of concealed social network activities based on communication technology choices: Early-warning detection of attack signals from terrorist organizations. Computational Math Organizational Theory, DOI 10.1007/s10588-009-9058-2.

5. Tang, J., Sun, J., Wang, C. & Yang, Z. (2009). Social influence analysis in large-scale networks. ACM Proceedings: KDD 09, June 28- July 1, Paris, France.

6. Tang, J., Musolesi, M., Mascolo, C. & Latora, V. (2009). Temporal distance metrics for social network analysis. ACM: WOSN 09 Proceedings, August 17, 2009, Barcelona, Spain.

7. Kang, H., Getoor, L. & Sing, L. (2007). Visual analysis of dynamic group membership in temporal social networks. SIGKDD Explorationa Newsletter, December 2007, Vol 9, Iss 2.

8. Yager, R. R. (2008). Intelligent social network analysis using granular computing. International Journal of Intelligent Systems, Vol 23, 1197-1220.

KEYWORDS: social networks, temporal aspects, conceptual extraction, visualization techniques, social graphs, algorithms

OSD10-L02 TITLE: Multi-sensor Extraction for Social Network Analysis - Tactical

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Provide a technology application suitable for tactical decision makers that can draw social network associations among people, objects, and locations from large and poorly formatted databases. These databases should include multi-sensor data feeds to include text and biometric data.

DESCRIPTION: A software prototype capable of ingesting multi-source data (text, biometrics) to produce social network relationships and predict high value targets (may be persons, objects, or locations). Social network algorithms that are adapted to large data sets and highly uncertain data will serve to structure knowledge for discovery. A visualization capability for these large and poorly structured networks will improve layered analysis and interpretation, and improve prediction for decision support. The focus of this research should be for the tactical level (edge) analyst who requires quick analysis of information from various sources for predictive decision making.

Tactical Warfighters demand rapid information fusion capabilities to develop and maintain accurate situational awareness and understanding of dynamic enemy threats in asymmetric military operations. The ability to extract meaning in relationships between people, objects, and locations from a variety of text and multi-source datasets is critical to proactive decision making at the Brigade and below level. These data reflect reality in an abstract and uncertain way; requiring novel algorithms for deriving mission-relevant information from soft (uncertain) intelligence sources. The software derivation of factors that will support discovery of relationships among people, objects, and places must be supported by experts in social network analysis who can lead the development of new graph matching techniques and visualization applications. New algorithms that support visual interpretation of associations in the data are needed due to the complexity of interactions among component parts, the dynamic nature of the relationships, and the short time periods available for analysis and decision making.

Fusion of uncertain and multi-source information is attracting a growing interest of practitioners and researchers [1, 2, 3, 4, 5]. The poor quality of the data stems from the quantity (far in excess of what a human analyst can process), the uncertainty or noisy features of the data (contain errors, inconsistencies, and potential deceptions), and the incomplete and ambiguous (can be interpreted in many different ways). Social network analysis techniques are frequently one output of this fusion process and are an aid to understanding complex relationships. However, as the corpus of information input increases and the quality of the data decreases, the resulting social network graphs will also become more complicated and difficult to analyze. To that end, a final challenge is to develop new algorithms to produce meaningful social networks for predictive analysis.

Challenges for this topic include 1) developing methods to discover and exploit information in poor quality and large datasets, 2) new algorithms for finding associations in data that show relationships between people, objects, and locations, 3) developing prototype software to portray these relationships to structure knowledge for discovery, 4) development of metrics to assess the correctness of extracted relationships compared to ground truth, and 5) the development of a validation testbed to demonstrate the automated knowledge representation against ground truth.

The focus of this effort involves structuring information for knowledge extraction based on the development of innovative algorithms to portray social networks from uncertain data. Several large unclassified datasets will be made available to the contractor to develop these prototype software services, algorithms, and social networks. The OSD is interested in innovative R&D that involves technical risk. Proposed work should have technical and scientific merit. Creative solutions are encouraged.

PHASE I: Complete a literature review, feasibility study and research plan that establishes the proof of principle of the approach for analyzing large datasets with a text/biometric software extraction tool capable of producing social network graphs that use novel algorithms. Identify the critical technology issues that must be overcome to achieve success. Prepare a revised research plan for Phase 2 that addresses critical issues.

PHASE II: Produce a prototype system that is capable of producing meaningful social network graphs from a corpus of uncertain data that can provide meaningful prediction of human behavior in relation to associated people, objects, and locations. The prototype should lead to a demonstration of the capability. Test the prototype in at least two environments with two different contexts. Demonstrate a capability to construct social network graphs using novel algorithms that support analytic knowledge discovery in dynamic time periods.

PHASE III: Produce a system capable of deployment in an operational setting of interest. Test the system in an operational setting in a stand-alone mode or as a component of larger system. The work should focus on capability required to achieve transition to program of record of one or more of the military Services. The system should provide metrics for performance assessment.

REFERENCES:
1. D.CER.2010.XX/ Advanced All Source Fusion ATO proposal, CERDEC-I2WD.

2. J. Biermann, Some Experiences with Experimental High Level Fusion Systems, FGAN-FKIE, Wachtberg, Germany.

3. James Llinas, Sambhoos, Little, Graphical Methods for Real-Time Fusion and Estimation with Soft Message Data, Proceedings Fusion 2008 Conference.

4. Pravia, M.A. Prasanth, R.K. Arambel, P.O. Sidner, C. Chee-Yee Chong, Generation of a fundamental data set for hard/soft information fusion, 11th International Conference on Information Fusion, 2008.

5. M. Sudit et al., A Graph-Based Framework for Fusion: From Hypothesis Generation to Forensics, the 9th Int'l. Conference on Information Fusion, Florence, Italy, 2006.

KEYWORDS: social networks, multi-source data extraction, relational algorithms, information fusion, large uncertain data sets

OSD10-L03 TITLE: End to End Analysis of Information Architectures

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Provide an end to end top down driven system analysis capability that would support management and control of errors in large data handling architectures.

DESCRIPTION: Development and use of a tool that enables understanding and control of errors arising from end to end processing of all data sources including sensor, multi-INT, and open source data within a specified large data handling architecture and that can support an arbitrary large data handling architecture.

Future large data handling architectures are anticipated to be composed from modules that perform specific functions in a particular way. These information architectures will support a wide variety of military and intelligence applications. It is expected that the modules form information architecture could be composed in a number of ways from a library of components. These architectures will be evaluated with regard to functional performance in a mission or variety of missions' as well as internal metrics such as computational resources required or memory storage. In development individual modules will also be evaluated with regard to performance and resource requirements in isolation. However, a capability that provides an end to end analysis of the complete information architecture, particularly with regard to a top-down viewpoint is lacking.

As an illustrative example consider a typical process for inferring intent might consist of ingesting a video sequence, detecting objects, identifying objects, defining tracks, activities, events, and combining this information with other data sources to infer intent. Processes flow such as the one described above will composed of modules each of which has a characterized performance. Often a system will be instantiated by using best of breed algorithms that might be computationally expensive with the hope that improvements in low level processing will automatically lead to improvements in higher level functions. This approach generally does not yield optimal solutions. This is not surprising since the large data handling system once it has been instantiated is a non-linear dynamical system. As is well known, non-linear dynamical systems may or may not be stable to small perturbations.

As a second example consider a system that performs object identification by detecting specific features. Clearly a number of features might be incorrectly detected or identified by low level processes, while the higher level function

yields the appropriate answer. For example, consider a system that identifies buildings that has been composed out of a system that identifies doors, windows, balconies, vents, and other building features. It is often the case that missed or incorrect identification of windows will not impact the performance of the building identification function. Hence, a more relevant question is given that the system performance at the highest level is to be controlled how should the system be composed to meet or control the high level requirement derived from the highest level of the mission and how should this be allocated to lower level processes and which, if any of the lower level processes significantly impact the higher level function.

Challenges for this topic include 1) developing methods for the analysis of arbitrary large data handling systems that implement the complete JDL Fusion process that model end to end performance, 2) development of methods that rapidly and accurately within a specific architecture identify performance limiting components or process steps, 3) methods that can support rapid evaluation of end to end performance as modules are changed, and 4) methods and strategies for identifying maximal errors for any module while guaranteeing end to end performance of the system to a specified error.

The focus of this effort is two fold and involves develop principled methods that enable control and management of large data handling system performance while simultaneously providing a tool that can support architecture and module assessment.

The OSD is interested in innovative R&D that involves technical risk. Proposed work should have technical and scientific merit. Creative solutions are encouraged.

PHASE I: Complete a feasibility study and research plan that establishes the proof of principle of the approach for creating a tool that can analyze an arbitrary large data handling architecture. Identify the critical technology issues that must be overcome to achieve success. Prepare a revised research plan for Phase 2 that addresses critical issues.

PHASE II: Produce a prototype system that is capable of analyzing an arbitrary large data handling architectures that perform the same function. Test the prototype tool with at least two large data handling environments. Demonstrate the capability to identify performance limiting or modules or modules that most significantly contribute to the overall error in the end to end system.

PHASE III: Produce a system capable of analyzing a deployed large data handling information architecture in an operational setting of interest. The work should focus on capability required to achieve transition of the analysis capability to programs of record of one or more of the military Services. The system should provide metrics for performance assessment and identification of components and modules that require additional research.

REFERENCES:

1. J. Esteban, A. Starr, R. Willets, P. Hannah, P. Bryanston-Cross “A Review of data fusion models and architectures: towards engineering guidelines”, Neural Comput. & Applic 14, 273-281 (2005)

2. W.M. Haddad and V. Chellaboina, Nonlinear Dynamical Systems and Control: A Lyapunov-Based, Approach, Princeton University Press, Princeton, NJ (2008)

3. J Sacks, W. J. Welch, T. J. Mitchell, and H. P Wynn, “Design and Analysis of Computer Experiments”, Statistical Science, Vol. 4, No. 4, 409-423, 1989

4. Aharon Bar-Hillel, Tomer Hertz, Daphna Weinshall: Object Class Recognition by Boosting a Part-Based Model. CVPR (1) 2005: 702-709.

5. A. Torralba, K. P. Murphy, W. T. Freeman and M. A. Rubin, “Context-based vision system for place and object recognition”, IEEE Intl. Conference on Computer Vision (ICCV), Nice, France, October 2003.

KEYWORDS: system analysis, design of experiment, non-linear dynamical systems, information architecture

OSD10-L04 TITLE: Automated Scene Understanding

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop technologies to represent data, information, and knowledge and to use it algorithmically to analyze, understand, compute, and reason under uncertainty.

DESCRIPTION: Mathematically grounded methods for capturing and representing qualitative variables such as topology, orientation, shape, proximity, similarity, and their measurement that enable computation and reasoning with qualitative information and its associated uncertainties, and fusing quantitative and qualitative information.

Fundamental advances in theoretical and statistical frameworks for data mining and data fusion have been made during the past few decades. Knowledge representation and reasoning have reached a level of sophistication that they can be applied to simple, controlled information integration and learning situations. A number of questions remain open and new questions have arisen, motivated by the opportunities and challenges in the cyber-physical space. In particular a representation for data that is both quantitative and qualitative at different levels of granularity, described over a network graph, efficient, supports fusion and reasoning is not known. Desirable characteristics in a representation handle the growing massive volume of data and increasing diversity of data types with different temporal characteristics, different physical attributes, different trustworthiness, and uncertainty. They would also support computation and reasoning using data with different uncertainties and information provenance. Finally it would be desirable if the information architecture and system in which the data, information, and knowledge is stored would be self aware and capable of assessing shortfalls in its knowledge including contradictory and incomplete data, knowledge or storage and suggest courses of action that are consistent with mission objectives to resolve these issues.

Decision-making is an optimization process that takes advantage of the available data and knowledge while mitigating its uncertainties. All sources of data and information and knowledge have their uncertainties regardless of source. All data is subject to timeliness, relevance, incompleteness, distortion, compromise, manipulation, and error. Scalability, extensibility, timeliness, relevance, usability, and higher cognitive-like abilities for reasoning still cut across all aspects of the decision-making process. Decision-making in the tactical environment is further complicated by the many separate but networked systems involved with decision-making at all levels of command.

Challenges for this topic include 1) Capturing and representing qualitative variables such as topology, orientation, shape, proximity, similarity, and their measurement, 2) Computing and reasoning with qualitative information and its associated uncertainties, and fusing quantitative and qualitative information, 3) Understanding the information content derived from observations of networks and sub-networks of sensors of varied configuration and modality 4) Building new models for ubiquitous association of entities and information.

The focus of this effort is two fold and involves the development of mathematically sound representations of data, information, and knowledge that support computation and reasoning, and employing these techniques.

The OSD is interested in innovative R&D that involves technical risk. Proposed work should have technical and scientific merit. Creative solutions are encouraged.

PHASE I: Complete a feasibility study and research plan that establishes the proof of principle for the representation of structured and unstructed data, information, and knowledge that supports reasoning and computation. Identify the critical technology issues that must be overcome to achieve success. Prepare a revised research plan for Phase 2 that addresses the identified critical issues.

PHASE II: Produce a prototype system that is capable of representing structured data obtained from sensors with known noise characteristics accompanied by metadata that is incomplete and imprecise, unstructured open source text data of unknown provenance, and multi-INT data with sensor errors and complete meta data. Demonstrate computation and reasoning over the data, information, and knowledge in particular performing inference and identification of gaps, conflict, and contradiction in the collection,. The prototype should lead to a demonstration of the capability.

PHASE III: Produce a system capable of deployment in an operational setting of interest. Test the system in an operational setting in a stand-alone mode or as a component of larger system. The work should focus on capability required to achieve transition to program of record of one or more of the military Services. The system should provide metrics for performance assessment.

REFERENCES:
1. F. Van Harmelen, V. Lifschitz, B. Porter, Handbook of Knowledge Representation, Elsevier, Amsterdam, The Netherlands (2008)

2. D. Blei, A. Ng, and M. Jordan (2003). "Latent Dirichlet allocation". Journal of Machine Learning Research 3: 993–1022 (2003)

3. Z. Wang, D. Zhang, A Li, X. Huang, and H. Peng, "Approach Comparison on Context-Aware Computing with Uncertainty", Technologies for E-Learning and Digital Entertainment", Springer-Verlag, Berln, (2007)

4. S. Lafon, Y. Keller, and R. R Coifman, "Data Fusion and Multicue Data Matching by Diffusion Maps. IEEE Trans. Pattern Anal. Mach. Intell. 28, 11 (Nov. 2006), 1784-1797.

KEYWORDS: data representation, information representation, knowledge representation, computing with uncertainty

OSD10-L05 TITLE: Shaping Sensor Data for Exploitation

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Provide a system that organizes and delivers mission relevant information from a multi-source sensor input

DESCRIPTION: A modular populated information architecture that accepts multi-source sensor data and processed information and organizes understands and summarizes that data/information on behalf of the warfighter. The architecture should consider services for (1) semantic metadata tagging (2) data organization enabled by a common data representation (3) space, time and content retrieval services (4) plain language summarization and delivery.

As the Department of Defense increases the capability and capacity to generate increasing amounts of data and information from the numerous sensors in the battlespace, the issue of handling very large data sets has become more challenging. This is in part due to Department of Defense response to a changing threat environment where there is an expansion of the types of sensors deployed, new types of information collected, and different features used to classify these new threats. From a technical perspective, sensor processing speeds have outpaced the speed and ability to transport, store and process the data created.

Challenges for this topic include 1) development of a common information space that multi-source data can be written to 2) development of space, time and content search utilities required to define and populate information cubes 3) development of services capable of auto-summarizing what is known about a space/time/content cube for rapid delivery to a bandwidth disadvantaged warfighter. The overall goal of the topic, enabled by the maturation of a common information space, is to rapidly deliver a fused situational awareness data to a tactical warfighter.

The common information space, in addition to being able to accept and organize multi-source data, must automatically tag data that describes the relevance of the data to a warfighter. Older data is often less relevant than newly collected data. Strategic information can have little relevance to the execution of a tactical mission. Information retrieval engines need to accept plain language requests such as "find relevant information to a specific mission type being executed within a specified area of interest as a specific time". A distributed architecture is required as many data sources are not easily moved due to limitations in available bandwidth on the battlespace.

An automated summarizer must package and deliver information discovered in the layered common information

space in a manner relevant to a preoccupied agile warfighter. The compression of many layers of multi-source data into an "information cube" and the automatic creation of a plain language summary describing the content contained within will require an ontology that links missions to areas within the common information space, semantic role labeling of unstructured text and is enabled by the use of meaningful data tags.

The OSD is interested in innovative R&D that involves technical risk. Proposed work should have technical and scientific merit. Creative solutions are encouraged. In addition to the research and development of technology and approaches, it is important to evaluate the impact of these efforts areas with regards to the way they change how large data sets are handled.

PHASE I: Complete a feasibility study and research plan that will mature an approach for creating plain language and mission relevant text summarizations of large data holdings enabled by a common information space. Identify the critical technology issues that must be overcome to achieve success. Technical work should focus on the reduction of key risk areas. For a constrained information space size, demonstrate that phase 1 risk reduction work has shown that a full implementation of the approach is technically tractable. Prepare a revised research plan for Phase 2 that addresses critical issues.

PHASE II: Produce a prototype system that is capable of producing plain language, mission relevant summarizations of a highly layered common information space. The prototype should enable a demonstration of the capability to be conducted using relevant data sources. The prototype should be relevant to multiple mission types, conducted in diverse environments.

PHASE III: Produce a system capable of deployment in an operational setting of interest. Test the system in a relevant setting in a stand-alone mode and as a component of larger system (programs of record). The work should focus on capability required to achieve transition to program of record of one or more of the military Services. The system should provide metrics for performance assessment.

REFERENCES:
1. Maria Lee. "Universal Core Advances Information Sharing Across Government Agencies". The Mitre Digest, November 2009

2. Dandashi, Higginson, Hughes, Narvaez, Sabbouh, Semy, Yost. "Common Vocabulary for Tactical Environments". Mitre Technical Report, 2007

3. B Schaffner. "Data Cubes Offer a New Dimension for Analyzing Information". http://articles.techrepublic.com.com/5100-10878_11-1046008.html?tag=content;leftCol

KEYWORDS: Ontology, Semantics, Semantic Search, Natural Language Processing, Machine Understanding, Database, Fusion

OSD10-L06 TITLE: Knowledge Discovery using Mobile Devices

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: The objective is to provide technology to automatically discover objects in a scene and perform a context-based assessment for mobile users. The capability should support hands free operation for military personnel engaged in field.

DESCRIPTION: An operational need exists to better support tactical users in knowledge discovery that is specific to information seen or heard in their area of operation. Military operators are engaged in activities that may require hands free operation of devices (voice or other I/O). New mobile devices feature GPS for location, network connectivity and numerous applications (apps). It is desired to use devices as digital assistants to make operators aware of significant entities or events in their area of operations and alert them to dangers. Devices need to ingest imagery and sounds (from warfighter mounted or proximity sensors), identify entities and behaviors within a scene,

automatically send entity/behavior knowledge representations to the ISR enterprise, provide for the discovery of knowledge in the enterprise relevant to the knowledge representation and for the display of discovered information on retrieved imagery that is aligned to warfighter position and heading. The handheld system needs to describe objects or behaviors with sufficient clarity to allow related information, including cultural data, held within the ISR enterprise to be discovered. Upon receipt of entity/behavior contextual information, the handheld system needs to display tactically relevant context on location and heading registered imagery which can be displayed on a mobile device. Algorithms need to be developed that can filter displayed information based on operator mission tasking.

The Department of Defense deals with very large quantities of data and requires methods to rapidly assess information relevant to users. Mobile devices such as iPhone and Android offer mobile computing assistance and communications. However, these devices need to be adapted for military environments. Mobile devices offer direct or indirect contextual awareness of surroundings. Indirect awareness occurs by means of networks and direct awareness by means of sensor or user device inputs.

Challenges for this topic include 1) entity (e.g. location, vehicle, weapon fire, facility) and behavior (e.g. crowd, clan symbol, loitering) recognition in scenes, 2) translation of images/sounds to knowledge objects that can be understood by a larger ISR enterprise 3) space/time/context based knowledge retrieval on received knowledge objects, 4) display of context data on location and heading registered imagery on a mobile device, and 5) keeping the warfighter and area sensors in a common coordinate (space and time) system. A mature system should make effective use of direct and indirect sources of information to maintain a current state of awareness in a dynamic data environment.

Technology needs to be developed to allow a warfighter tactical device to convey scene understanding, add context and display a composite view to the tactical warfighter. Focus of the topic is on bandwidth constrained expeditionary warfighters. The vision is to provide a personal digital assistant that will make the user aware of relevant visually oriented critical information in a changing environment by enabling an accurate representation of the environment to be transmitted to the ISR enterprise. The goal is to greatly increase the effective utilization of large data stores. User safety in dangerous and unfamiliar areas is of the highest priority. The system should automatically generate alerts such as “building ahead is associated with terrorist activity,” “entering area of recent RPG attack,” and “explosion detected 1 km north by an overhead sensor”.

The OSD is interested in innovative R&D that involves technical risk. Proposed work should have technical and scientific merit. Creative solutions are encouraged.

PHASE I: Complete a feasibility study and research plan that leads to a matured technical approach and a successful proof of principle demonstration for hands free operations of mobile devices for military users. Identify the critical technology issues that must be overcome to achieve success and track key risk reduction activity. Prepare a research plan for Phase 2 that addresses critical issues for prototyping.

PHASE II: Produce a prototype system that is capable of producing context based spatially oriented information assistance and operator alerts. Demonstrate device operation in a hands free mode (e.g. voice, sign or other means). Test the device in a lab setting in two or more contexts. Develop a concept of operation in support of a specific user community with potential situational dangers and need of assistance alerts. Outline methods to incorporate input from smart area EO/IR and acoustic sensors. The prototype will need to track area sensors and the warfighter in a common coordinate system. The existence of a searchable enterprise knowledge store can be assumed.

PHASE III: Produce a system capable of deployment in an operational setting. Test the system in an operational setting in a stand-alone mode and as a component of larger network. The work should focus on capability required to achieve transition to program of record of one or more of the military Services. The capability should use open standards and military guidance for net-centric operations. Performance metrics should be defined with the transition program partner and assessment made.

REFERENCES:

1. Data Sharing in a Net-Centric Department of Defense, DoD Directive No. 8320.2, Dec 2, 2004.

2. B. Sutherland, “Apple’s New Weapon To help soldiers make sense of data from drones, satellites and ground

sensors, the U.S. military now issues the iPod Touch". Newsweek April 2009. http://newsweek.com/id/1945623

3. Prince McClean, "Inside Google's Android and Apple's iPhone OS as core platforms", Nov 5, 2009.

4. H. W. Gellersen, A. Schmidt and M. Beigl, "Multi-Sensor Context-Awareness in Mobile Devices and Smart Artifacts", Mobile Networks and App. 7, 341–351, 2002.

KEYWORDS: knowledge discovery, augmented reality, human-computer interaction

OSD10-L07 TITLE: Data Discovery for Exploitation from Distributed Sources

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: To seek an innovated technology that will enable handling massive datasets from relational databases and further processing, discovering of relevant information in a distributed or parallel fashion to increase analytic throughput.

DESCRIPTION: This BAA seeks a modular component that can be part of a future end-to-end system with capability of distilling, analyzing, discovering, structuring, and interpreting relevant information hidden in data that is already stored in relational databases. Although data is already organized with the help of attributes and their associated keys, more meaningful information can still be culled from the dataset. Relevant information hidden in data often exists at different spatio-temporal scales in which various features/descriptors must be discovered, described or summarized. To gain further insight, one can attempt to hierarchically assemble these descriptors to form multi-layers of interpretation or abstraction.

Moreover, this BAA emphasizes the exploitation of distributed or parallel computation to speed up the processing tasks mentioned above, especially in handling massive datasets. Recent advances in numerical procedures and fast algorithms have generated a suite of new tools that are indispensable in handling and processing digital data.

From the R&D perspectives, the proposed undertakings must be grounded on the results from Basic or Applied Research within the last five years. In addition, the algorithmic designs must be based on rigorous or provable principles of mathematics, statistics, and computer science.

Besides the aforesaid requirements, the technology should provide the following capabilities:

1. Automatic extraction and tracking of pertinent descriptors together with their statistical characteristics as the dataset evolves through time.
2. Multi-scale interpretation and hierarchical analysis of discovered descriptors (objects, clusters, outliers, etc.) which tend to appear within various spatio-temporal scales or persist across scales. The scale parameters should be mostly automatically tuned by rigorous procedures and not be determined by trial and error.
3. Efficient and intelligent query, retrieval and its ranking - beyond simple search by keywords or database attributes - which employ the structure of descriptors discovered above and database schema.
4. Acceptance of user's input for query and retrieval refinement in case the initial query results do not contain sufficiently relevant information.
5. Robustness to noisy, missing data, and the choice of metrics being used to analyze data at various stages.
6. Ingesting data from a variety of DoD's applications.

This BAA is part of a larger effort to discover information hidden in structured data by combining the existing structures or relations among metadata with the new techniques equipped to analyze unstructured data. The OSD is interested in innovative R&D that involves a degree of technical risk. Creative solutions are highly encouraged.

PHASE I: Initiate a feasibility study that establishes the proof of principle of a design that can handle large, structured data from relational databases for shaping data for exploitation. Devise a distributed or parallel computational architecture that can speed up implementation of sophisticated algorithms. Identify the critical

technology issues or gaps that need to be solved to achieve objectives.

PHASE II: Complete the research plan in Phase I. Produce a prototype system that provides a data discovery tool for exploitation. The prototype should lead to a demonstration of the capability. Test and demonstrate the prototype's capability in at least two different applications from multiple databases.

PHASE III: Produce a system capable of deployment in an operational setting of interest. Test the system in an operational setting in a stand-alone mode or as a component of larger system. The work should focus on capability required to achieve transition to program of record of one or more of the military Services. The system should provide metrics for performance assessment.

REFERENCES:
1. M. Mahoney, L.-H. Lim, and G. Carlsson "MMDS 2008: Algorithmic and Statistical Challenges in Modern Large-Scale Data Analysis, Part I", SIAM News, Volume 42, Number 1, 2009.

2. M. Mahoney, L.-H. Lim, and G. Carlsson "MMDS 2008: Algorithmic and Statistical Challenges in Modern Large-Scale Data Analysis, Part II", SIAM News, Volume 42, Number 2, 2009.

3. G. Carlsson, "Topology and Data," Bulletin of the American Mathematical Society, vol 46, Number 2, pp.255-308, 2009.

4. G. Golub, M. Mahoney P. Drineas, and L.-H. Lim, "Bridging the gap between numerical linear algebra, theoretical computer science, and data applications", SIAM News, Volume 39, Number 8, 2006.

5. Y. Yao, J. Sun, X. Huang, G. Bowman, G. Singh, M. Lesnick, L. Guibas, V. Pande, G. Carlsson, "Topological methods for exploring low-density states in biomolecular folding pathways ," The Journal of Chemical Physics April 2009.

6. V. Rokhlin, M. Tygert, "A Fast randomized algorithm for over-determined linear least-squares regression", PNAS, 105 (36): 13212 – 13217, 2008.

KEYWORDS: Massive dataset; relational database; distributed computation; parallel computation; unstructured data

OSD10-L08 TITLE: Real-time Resource Allocation Co-Processor

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Design, develop, and test an optimization co-processor to enable real-time resource allocation

DESCRIPTION: The long range challenge is to efficiently allocate complex computing tasks among small but powerful wireless mobile computing devices. Recent advances in computer technology are creating opportunities for more intelligent decisions in the field. While there is a long history of solving complex problems using the power of modern computing machinery, there is growing need to solve tasks involving information and decision processing in the field, close to where events are actually happening. Meanwhile, there is a growing number of small but surprisingly powerful computing devices becoming available. While these units can not individually compete with the power of a large central computer, they can communicate and work together.

An important goal is to put information processing closer both to the source of information as well as the people who need to use the information. Although wireless mobile computers are becoming increasingly powerful, they are small and even when aggregated they are not up the task of optimizing resource allocation, while performing the associated decision processing tasks.

By drawing on the collective capability of the multiple computers that are within communications range of each

other, the challenge is that there is more than one sensor that may be collecting data and other computers may have their own sensor data to work on. But we can exploit the property that much of the data collected is redundant with previously collected data. When one computer encounters a burst of potentially important data, it might be possible to pre-empt a nearby computer, sending it data (and possibly algorithms) that contain potentially important information needing to be processed now!

Challenges for this topic include 1) developing architecture to enable real-time resource allocation that includes optimization, such as simplex, change point detection, together with adaptive filtering, to help in the identification of potentially important data 2) designing, developing, and testing an optimization co-processor.

The focus of this effort is to design, develop, and test a hardware co-processor to enable real-time resource allocation.

The OSD is interested in innovative R&D that involves technical risk. Proposed work should have technical and scientific merit. Creative solutions are encouraged.

PHASE I: Complete a feasibility study, research plan, and initial design that establishes the proof of principle of the approach for a real-time resource allocation co-processor that includes optimization, change point detection, and adaptive filtering, to optimize real-time resource allocation, while identifying critical technology issues that must be overcome to achieve success. Prepare a revised research plan for Phase 2 that addresses critical issues.

PHASE II: Refine design, develop, and test a prototype system that is capable of optimizing computational resources through the use of optimization, change point detection, and adaptive filtering. The prototype should lead to a demonstration of the capability. Test the prototype in at least two environments with two different contexts.

PHASE III: Produce a system capable of deployment in an operational setting of interest. Test the system in an operational setting in a stand-alone mode or as a component of larger system. The work should focus on capability required to achieve transition to program of record of one or more of the military services. The system should provide metrics for performance assessment.

REFERENCES:
1. J. Chen and A. Gupta, Parametric Statistical Change Point Analysis, Birkhauser, Boston, MA, 2000.

2. D. Pados and G. Karystinos, “An Iterative Algorithm for the Computation of the MVDR Filter,” IEEE Transactions on Signal Processing, Vol. 49, pp.290-300, February 2001.

3. J. A. Shapiro and W. B. Powell, “A Metastrategy for Large-scale Resource Management Based on Informational Decomposition, Informs Journal on Computing, Vol. 18, pp.43-60, 2006.

KEYWORDS: optimization, change point detection, adaptive filtering, real-time resource allocation

OSD10-L09 TITLE: Framework for Large Streaming Data Analysis

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Provide a scalable framework for ingesting, analyzing and distributing streaming audio and video data to support various DoD needs.

DESCRIPTION: A scalable framework that allows disparate formats, analysis algorithms, ingestion systems, and presentation systems to be integrated in a loosely coupled fashion to exploit large amounts of streaming audio and video data.

Many current DoD Command and Control and ISR systems are of a typical stovepipe design that does not allow for horizontal integration of functionalities and data. The DoD is moving away from this approach and going a more

modular and pluggable design. In the past, many streaming media workflows were designed with the intent of addressing a specific need and without requirements to be interoperable or modifiable on the fly. This framework will change that.

In order to provide warfighters with the correct and relevant information in a timely fashion, this framework will expose interfaces for the analysis algorithms, ingestion systems and distribution methods. It will also provide for the mediation of formats. Together this will allow a user to run any analysis algorithms on a stream from any source and present it to any consumer. Such workflows will be made available for consumption by other analysts. Workflows that are already established, formalized and vetted as business processes will also benefit from this. The system will provide a functionality to convert business processes to executable workflows. This will eliminate some of the manual conversion and integration in these processes, while keeping the processes as they were formalized.

This topic presents several challenges. Many of them fall under the category of interoperability issues and include such items as: mediating between formats without information loss and exposing interfaces to analysis algorithms, ingestion systems, and distribution systems to make them pluggable. In addition such a framework will need to be scalable. New algorithms, formats, and data sources should be easily added. Scalability will also extend to the ability to support highly complex workflows and large numbers of streaming data sources. It is also expected to conform to established standards used by the DoD and industry.

The OSD is interested in innovative R&D that involves technical risk. Proposed work should have technical and scientific merit. Creative solutions are encouraged.

PHASE I: Complete a systems architecture design and engineering plan. Identify the gaps and pitfalls in designing a system with the currently available technology. Establish approaches to meet these gaps and avoid these pitfalls.

PHASE II: Complete a prototype system that demonstrates the ability to work with several formats, analysis algorithms, ingestion systems, and presentations systems in a basic ISR workflow. The system should also demonstrate the ability to be scaled so that other functionalities may be added with limited time and development cost.

PHASE III: Complete a deployable system that is capable of functioning in an operational environment. Test the system in the operational setting and provide performance metrics for said system. Metrics should indicate the ability to function in an operational environment. Functional requirements necessary to transition to one of the military Services should also be evaluated.

REFERENCES:

1. J. A. Ballas and J. Nevitt. "Using Web Services to Foster Global Collaboration in Sound Design." Proceedings of the 14th International Conference on Auditory Display, Paris, France (2008).

2. H. Detmold, A. Dick, K. Falkner, D. Munro, A. van den Hangel, and R. Morrison. "MiddleWare for Distributed Video Surveillance." IEEE Distributed Systems Online. Feb. 2008.

3. H. Detmold, A. Dick, K. Falkner, D. Munro, A. van den Hangel, and R. Morrison. "Scalable surveillance software architecture." Proceedings of the IEEE International Conference on Advanced Video and Signal-based Surveillance (poster) (2006).

4. N. Dube, H. Bhatt, R. Ramakrishna, K.S. Dasgupta. "Service Oriented Architecture for Satellite Image Processing. " Proceedings of the 13th International Conference on Advanced Computing and Communications (ADCOM) (2005).

KEYWORDS: streaming video, streaming audio, analysis algorithms, scalable framework, ISR workflow, business process