RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)						DATE: February 2008	
APPROPRIATION/BUDGET ACTIVITY: RDT&E, Defense-wide; BA2 Applied Research			R-1 ITEM NOMENCLATURE: Information and Communications Technology; PE 0602303E				
COST (In Millions)	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Total Program Element (PE) Cost	228.073	230.385	254.009	234.676	203.437	201.456	201.454
High Productivity, High-Performance Responsive Architectures IT-02	84.927	65.913	98.641	85.764	67.360	67.360	67.359
Information Assurance and Survivability IT-03	72.607	93.049	80.349	76.479	83.484	81.503	81.502
Language Translation IT-04	70.539	71.423	75.019	72.433	52.593	52.593	52.593

(U) Mission Description:

(U) The Information and Communications Technology program element is budgeted in the applied research budget activity because it is directed toward the application of advanced, innovative computing systems and communications technologies.

(U) The High Productivity, High-Performance Responsive Architectures project is developing high-productivity, high-performance computing hardware and the associated software technology base required to support future critical national security needs for computationally-intensive and data-intensive applications. These technologies will lead to new multi-generation product lines of commercially viable, sustainable computing systems for a broad spectrum of scientific and engineering applications; it will include both supercomputer and embedded computing systems.

(U) The Information Assurance and Survivability project is developing the technology required to make emerging information system capabilities (such as wireless and mobile code/mobile systems) inherently secure, and to protect DoD's mission-critical systems against attack upon or through the supporting information infrastructure. These technologies will enable our critical systems to provide continuous correct operation even when they are attacked, and will lead to generations of stronger protection, higher performance, and more cost-effective security and survivability solutions scalable to several thousand sites.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E

(U) The Language Translation project will develop and test powerful new Human Language Technology that will provide critical capabilities for a wide range of national security needs. This technology will enable systems to a) automatically translate and exploit large volumes of speech and text in multiple languages obtained through a variety of means; b) to have two-way (foreign-language-to-English and English-to-foreign-language) translation; c) enable automated transcription and translation of foreign speech and text along with content summarization; and d) enable exploitation of captured, foreign language hard-copy documents.

(U) **Program Change Summary:** *(In Millions)*	**FY 2007**	**FY 2008**	**FY 2009**
Previous President's Budget	234.065	229.739	284.646
Current Budget	228.073	230.385	254.009
Total Adjustments	-5.992	0.646	-30.637
Congressional program reductions	0.000	-1.474	
Congressional increases	0.000	2.120	
Reprogrammings	0.000		
SBIR/STTR transfer	-5.992		

(U) Change Summary Explanation:

FY 2007	The decrease reflects the SBIR/STTR transfer.
FY 2008	The increase reflects reductions for Section 8097 Contractor Efficiencies and Section 8104 Economic Assumptions, offset by congressional adds National Repository of Digital Forensic Intelligence and Software Assurance Education and Research Institute.
FY 2009	The decrease reflects program re-phasing primarily in the Information Assurance and Survivability project, IT-03.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)						DATE February 2008	
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research			R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02				
COST (In Millions)	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
High Productivity, High-Performance Responsive Architectures IT-02	84.927	65.913	98.641	85.764	67.360	67.360	67.359

(U) Mission Description:

(U) The High Productivity, High-Performance Responsive Architectures project is developing high-productivity, high-performance computer hardware and the associated software technology base required to support future critical national security needs for computationally-intensive and data-intensive applications. These technologies will lead to new multi-generation product lines of commercially viable, sustainable computing systems for a broad spectrum of scientific and engineering applications; it will include both supercomputer and embedded computing systems. The project will ensure accessibility and usability to a wide range of application developers, not just computational science experts. This project is essential for maintaining the nation's strength in both supercomputer computation for ultra large-scale engineering applications and for surveillance and reconnaissance data assimilation and exploitation.

(U) One of the major challenges currently facing the DoD is the prohibitively high cost, time, and expertise required to build large complex software systems. Powerful new approaches and tools are needed to enable the rapid and efficient production of new software, including software that can be easily changed to address new requirements and can adjust dynamically to platform and environmental perturbations.

(U) Even as this project develops the next generation of high-productivity, high-performance computing systems, it is looking further into the future to develop the technological and architectural solutions that are required to develop "extreme computing" systems. The military will demand increasing diversity, quantities, and complexity of sensor and other types of data, both on the battlefield and in command centers - processed in time to effectively impact warfighters' decisions. Computing assets must progress dramatically to meet significantly increasing performance and significantly decreasing power and size requirements. Extreme computing systems will scale to deliver a thousand times the capabilities of future petascale systems using the same power and size or will scale to deliver terascale-embedded systems at one millionth of the size and power of petascale systems. The resulting extreme computing systems will be capable of scaling from embedded to leadership class systems. The most significant technical achievements that must be realized to obtain the goals of extreme computing are the enabling architectural advancements, pervasive low power technologies, and low volume physical packaging of these systems. Numerous additional technical challenges must be resolved, including the reliability of "extreme computing" systems: embedded systems require a higher level of reliability and assurance than general-purpose systems because the failure of an embedded computing system can result in the loss of a deployed platform.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02

(U) Program Accomplishments/Planned Programs:

	FY 2007	FY 2008	FY 2009
High-Productivity Computing Systems	77.952	47.243	71.654

*Previously part of Responsive Computing Architectures

(U) The ongoing High-Productivity Computing Systems (HPCS) program will enable nuclear stockpile stewardship, weapons design, cryptanalysis, weather prediction, and other large-scale problems that cannot be addressed productively with today's computers. The goal of this multi-agency program is to develop revolutionary flexible and well-balanced computer architectures that will deliver high performance with significantly improved productivity for a broad spectrum of applications.

(U) It is extremely difficult to program today's high-performance computers; even for expert programmers, these systems present a significant challenge. The programming of such large systems must be made much easier so that programmers and scientists with minimal computer skills can harness the power of high-performance computers. As the number of processors increases to 100,000 and beyond, it is difficult not only to develop application codes, but also to debug and optimize them, since tools that will help are designed for small-scale systems (10's of processors). This area of user productivity is where HPCS is focusing significant effort. The HPCS technology development plan is being executed in three phases that will extend to the end of this decade. The three phases are (I) concept design study, (II) research and development, and (III) system development, resulting in large-scale prototypes.

(U) Initiated in 2002, the DARPA HPCS program is responsive to a strategy developed in conjunction with the U.S. National Security Community. The ultimate goal of the HPCS program is to create a new generation of economically viable high productivity computing systems for the national security and industrial user communities. High productivity computing is a key technology enabler for meeting our national security and economic competitiveness requirements. In November 2006, the HPCS program moved into the third and final phase, with a down-select from three vendors to two. In Phase III of the HPCS program, the two remaining vendors will complete the designs and technical development of very large (petascale) productive supercomputers, with demonstration of prototype systems in 2010-2011. DARPA funding is sufficient to cover the contractual requirements of one of the two selected vendors. NSA and DOE, partners with DARPA in this program, provide funding to enable maintaining a second vendor in the program.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02

(U) Program Plans:

FY 2007 Accomplishments:

- Performed a down-select from the three HPCS Phase II participants to two Phase III participants.
- Initiated prototype development (Phase III) of two high-end high-productivity petascale computing systems.
- Initiated high-level design of key application-specific integrated circuits (ASICs) and development of hardware simulators.
- Performed research and development on parallel programming languages and/or development environments that will increase user productivity on HPCS systems, and released early versions of the languages to HPCS stakeholders.

FY 2008 Plans:

- Complete design verification of most ASICs: a critical step before releasing design to the very costly fabrication process.
- Develop and implement operating system scaling and performance improvements so that existing operating systems can be leveraged, saving development costs, facilitating use of legacy code, and improving user productivity by preventing the need to learn a new operating system.
- Demonstrate early versions of productivity tools for the HPCS stakeholders to solicit their feedback.
- Continue developing productivity tools.
- Conduct an HPCS software critical design review of each vendor.
- Vendor delivery of HPCS system design specifications for evaluation by the government.
- Explore opportunities to expand the user base for high-end computing.

FY 2009 Plans:

- Release of the beta version application development software to HPCS stakeholders for evaluation and provide familiarity with the software prior to system release thus reducing the learning curve upon system availability.
- Fabricate and test several of the ASICs.
- Continue to develop and implement operating system scaling and performance improvements.
- Continue developing productivity tools.
- Conduct critical design review of each HPCS vendor’s system.
- Begin porting applications to a subset of the actual HPCS prototype hardware in preparation for FY 2010 subsystem demo that will provide evidence that the full prototype system will meet its productivity and performance goals.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02

	FY 2007	FY 2008	FY 2009
Software Producibility	6.975	10.600	15.996

*Previously part of Responsive Computing Architectures.

(U) The Software Producibility program will reduce the cost, time, and expertise required to build large complex software systems. This includes new techniques for rapidly developing adaptive software that can be easily changed to conform to new software design and development tools, readily complies to new requirements, and readjusts dynamically to environmental perturbation. Today, production-quality compilers are developed at significant cost for a defined class of systems regardless of the actual system resources available to and/or needed by an application. This places significant programming burden on developers when creating applications who must consider the platform and its applications. Improvements in compiler technology can greatly simplify application development by providing the capability to automatically and efficiently generate a compiler that reliably executes a broad spectrum of military and industrial applications for target computing systems that range from a single multi-core processor system to very large multi-processor systems. Military systems critically depend on complex software that is reliable, robust, and secure. Mature software frameworks (e.g., Apple Cocoa, Microsoft Foundation Class library, Java Swing, JBOSS, SDL, etc.) provide well tested and well-considered mechanisms that, if used properly, can enable developers to quickly create sophisticated applications of high quality. But designers/developers have a very steep learning curve when working in a new framework. A combination of fundamental software analysis and tool assistance can enable software developers to function effectively at the expert level in multi-framework environments but without the excessive investments of time required by current techniques.

(U) Program Plans:

FY 2007 Accomplishments:

- Formulated a strategy for achieving software producibility through adaptivity.
- Identified challenge problems, in the flight control system and software radio domains, for evaluating new adaptive software techniques.
- Identified candidate strategies for rapidly employing existing, mature, software frameworks to speed new system construction.

FY 2008 Plans:

- Develop toolchains to support preliminary flight control/vehicle management system and software defined radio experiments.
- Conduct a fault management design time experiment.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02

- Conduct a software defined radio design time and load time adaptation experiments.
- Investigate an initial concept for characterization tools and self-assembling compiler elements.

FY 2009 Plans:

- Develop toolchains to support optimized verification, field update and security adaptation experiments.
- Conduct optimized verification, field update and security adaptation experiments.
- Create the initial common development environment and supporting technologies that will allow efficient application development, implementation, and execution on heterogeneous computer architectures.
- Develop inter-framework mappings and other techniques to make software expertise more portable to the "next" required framework.
- Develop tools and techniques that enable software developers to perform at the expert level in multiple complex software frameworks simultaneously.

	FY 2007	FY 2008	FY 2009
Extreme Computing *	0.000	8.070	10.991

*Previously part of Responsive Computing Architectures.

(U) The Extreme Computing program will enable ExaScale computing systems in the post-2010 timeframe, with processing that will exceed one quintillion (10^18) operations (floating point, fixed point or data movement), per second. Significant technical roadblocks to scalable performance, productivity, physical size, power, and programmability must be overcome to realize the goals of extreme computing. As Moore's law reaches its limit, we can no longer depend on significantly increasing clock rates for performance advances. Current and evolutionary bandwidth and latency of data movement operations and current data placement approaches will not be sufficient to sustain anticipated or desired increases in processing performance. It will be essential to find new techniques that minimize data movement and optimize data communication performance.

(U) Ensuring dramatic advances in processing performance is critical as the amount and type of raw data needing to be turned into actionable information rapidly escalates. Previously, advances in commercial off-the-shelf (COTS) systems have addressed these needs but future COTS processors are ill-suited for developing military requirements because they are increasingly less productive for military applications, are power-

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02

hungry, and limit the performance available to the warfighter. To support escalating processing needs both at the embedded and supercomputer level, completely new architectures at the processor/memory/data movement and system level are needed to enable extreme computing.

(U) Another critical research area will develop self aware, self optimizing processing system approaches. Within the context of DoD systems, mechanisms for self-modification will enable systems to adapt in real-time to changing requirements, faults, and malicious attacks. Research in self-aware trusted computing will develop the capabilities to provide autonomous system monitoring and optimization, ensuring the necessary processing system adaptations are transparent to the operator. Self-monitoring hardware in conjunction with co-developed software will incorporate cognitive techniques to determine the state, performance, and health of the processing system, and based on the processing system's self-evaluation, will reconfigure to provide optimized system performance.

(U) Program Plans:

FY 2008 Plans:

- Identify and assess the potential technologies necessary to provide the types of improvements essential to achieve extreme computing: non-von Neumann architectures; 3-D microelectronic structures; high bandwidth/low latency electrical and optical technologies, multiple-core processors; radically different packaging solutions; new memory and storage architectures; and non-intrusive interfaces.
- Formulate new processor and memory architectures that will lead to extreme computing.
- Initiate a study to identify potential new hardware architectures and candidate approaches, such as master/slave methods where the "slave" collects and condenses data.
- Develop initial concepts for, and evaluate the feasibility of computational architectures and computing systems that monitor execution at run time, and dynamically optimize performance (e.g., with respect to caching, on-chip packet routing, etc.) on common applications.

FY 2009 Plans:

- Develop the identified critical technologies, processor technologies, system methodologies, and architectures to enable general-purpose and embedded computing systems to perform at exascale levels and beyond and enable significantly improved and new capabilities to the warfighter.
- Explore, develop, evaluate and perform initial simulations of techniques to enable computing systems to self-monitor their state, identify unexpected or unwanted system behavior, marshal processing resources to optimize performance, and transparently adapt in real time.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02

– Establish initial coordination with selected DoD applications for self-aware/self-optimizing approaches to establish example DoD context and future transition opportunities.

(U) Other Program Funding Summary Cost:

- Not Applicable.

THIS PAGE INTENTIONALLY LEFT BLANK

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

COST (In Millions)	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Information Assurance and Survivability IT-03	72.607	93.049	80.349	76.479	83.484	81.503	81.502

(U) Mission Description:

(U) This project is developing the technology required to make emerging information system capabilities (such as wireless and mobile code/mobile systems) inherently secure, and to protect DoD's mission-critical systems against attack upon or through the supporting information infrastructure. These technologies will enable our critical systems to provide continuous correct operation even when they are attacked. The technologies will also lead to generations of stronger protection, higher performance, and more cost-effective security and survivability solutions scalable to several thousand sites. Technologies developed under this project will be exploited by all the projects within this program element, and those in the Command, Control, and Communications program element (PE 0603760E), the Network-Centric Warfare Technology program element (PE 0603764E), the Sensor Technology program element (PE 0603767E), the Guidance Technology program element (PE 0603768E), and other programs that satisfy defense requirements for secure, survivable, and network centric systems.

(U) Program Accomplishments/Planned Programs:

	FY 2007	FY 2008	FY 2009
Next Generation Core Optical Networks (CORONET)	7.841	14.000	14.500

(U) The Next Generation Core Optical Networks (CORONET) program will revolutionize the operation, performance, security, and survivability of the United States' critical inter-networking system by leveraging technology developed in DARPA photonics component and secure networking programs. These goals will be accomplished through a transformation in fundamental networking concepts that form the foundation upon which future inter-networking hardware, architecture, protocols and applications will be built. Key technical enablers that will be developed in this thrust include: (1) network management tools that guarantee optimization of high density wavelength-division-multiplexed optical channels, such as those provided by wavelength division multiplexing; (2) creation of a new class of protocols that permit the cross-layer communications needed to support quality-of-service requirements of high-priority national defense applications; and (3) demonstration of novel concepts in applications such as distributed and network based command and control, intelligence analysis, predictive logistics management,

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

simulation and scenario enhanced decision-making support for real-time combat operations, and assured operation of critical U.S. networking functions when faced with severe physical layer attack. These network-based functions will support the real-time, fast-reaction operations of senior leadership, major commands and field units.

(U) A complimentary effort, the Transmission, Switching and Applications for Next-Generation Core Optical Networks program will develop the technology and applications to realize the next-generation dynamic multi-terabit networks that can deliver advanced internet protocol and optical services. This will be accomplished by: (1) greatly increasing network capacity through the use of more efficient fiber-optical transmission techniques; (2) implementing agile, high capacity, all optical switching platforms, and (3) developing the software and hardware interfaces, as well as the migration strategy, to enable new applications that can take full advantage of dynamic multi-terabit core optical networks.

(U) Program Plans:

– Next Generation Core Optical Networks (CORONET)

FY 2007 Accomplishments:

-- Completed an extensive economic study of all-optical bypass and grooming at the core and the edge of a global fiber-optic network.

-- Completed a study of the capacity limits of digital, wavelength-division-multiplexed (WDM) fiber-optic transmission systems, which showed the potential for more than ten-fold increase in the capacity per fiber compared to today's systems.

-- Completed a study of analog WDM fiber-optic transmission systems, which showed that such analog systems are limited to distances of several tens of kilometers. Thus they are not suitable for core optical networks of national or global extent.

FY 2008 Plans:

-- Develop the architectures and define the network elements for a fast reconfigurable optical core network.

-- Develop protocols, algorithms and the network control and management architecture to provide fast service setup, fast restoration from multiple network failures and guaranteed quality of service for a global core optical network.

FY 2009 Plans:

-- Model and simulate a dynamically reconfigurable multi-terabit global core optical network.

-- Initiate the development of the network control and management software such that the final product will be transitioned and implemented in current commercial and DoD core optical networks.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

– Transmission, Switching and Applications for Next-Generation Core Optical Networks
FY 2007 Accomplishments:
-- Completed a study to determine the capacity limits of modern fiber telecommunications.
FY 2008 Plans:
-- Complete a study on the use of "Maximum Likelihood Sequence Estimation", to increase the spectral efficiency of existing optical networks by up to ten times.
-- Complete a study to determine the impacts of emerging 100 Gbps Ethernet technology on next-generation optical networks.
-- Initiate a study to examine migration strategies and associated software and hardware interfaces to enable new applications for next-generation core optical networks.
FY 2009 Plans:
-- Develop and demonstrate an efficient fiber-optical transmission technique to enable several-fold increase in fiber capacity.
-- Develop architecture design and fabrication of a multi-terabit all-optical switch capable of fast switching of wavelengths and of sub-wavelength grooming.
-- Develop the software and hardware interfaces, as well as the migration strategy, to enable new applications that can take full advantage of dynamic multi-terabit core optical networks.
-- Initiate a national-scale multi-terabit network testbed to test and demonstrate hardware, software and applications of next-generation core optical networks.

	FY 2007	FY 2008	FY 2009
Dynamic Quarantine of Computer-Based Worms	25.201	12.343	10.932

(U) The goal of the Dynamic Quarantine of Computer-Based Worms program is to develop defenses for U.S. military networks against large-scale malicious code attacks such as computer-based worms. As the U.S. military pushes forward with network-centric warfare, terrorists and other nation-states are likely to develop and employ self-replicating malicious code to impede our ability to fight efficiently and effectively. This program will develop the capability to automatically detect and inoculate DoD networks against never before seen computer worm attacks. This program will also assess the comparative strength of different architectural solutions.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

(U) The DCAMANET program developed and refined technologies for Defense Against Cyber Attacks on Mobile Ad-hoc Network Systems (DCAMANETS). This effort researched, prototyped, and evaluated defenses that sensed failures and attacks on military tactical wireless networks and auto-reconfigured in real-time to provide continuous service of mission-critical activities. The next step of the DCAMANET program will be to develop an intrinsically assurable mobile ad-hoc network. An intrinsically assurable mobile ad-hoc network will directly support integrity, availability, reliability, confidentiality, and safety of MANET communications and data. In contrast, the dominant Internet paradigm is intrinsically insecure. For example, the Internet does not deny unauthorized traffic by default and therefore violates the principle of least privilege. In addition, there are no provisions for non-repudiation or accountability and therefore adversaries can probe for vulnerabilities with impunity because the likelihood of attributing bad behavior to an adversary is limited. Current protocols are not robust to purposely induced failures and malicious behavior, leaving entire Internet-based systems vulnerable in the case of defensive failure.

(U) Program Plans:

– Dynamic Quarantine of Computer-Based Worms

FY 2007 Accomplishments:

-- Completed two prototype systems utilizing divergent methodologies.
-- Strenuously tested prototypes against self-replicating malicious code on simulated operational networks.
-- Refined prototypes automatic detection and quarantine mechanisms and prepared for further testing that will encompass nation-state level of worm attacks.

FY 2008 Plans:

-- Develop requirements to integrate system into DoD enterprise networks.
-- Integrate Defense Quarantine of Computer Based-Worms (DQW) prototype into DoD enterprise solution tool suite.
-- Harden system against directed attacks.
-- Conduct operational test of representative integrated system against full-spectrum nation state worm threat.
-- Test integrated system on operational representative network.

FY 2009 Plans:

-- Test integrated system against red teams (attack teams) during combatant command exercise.
-- Commence technology transition to DoD.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

– Defense Against Cyber Attacks on MANETS (DCAMANETS)
FY 2007 Accomplishments:
-- Prototyped, tested, and evaluated three DCAMANETS solutions.
-- Developed an automated mobile wireless testbed that emulates operational environments.
-- Developed and tested host-based and network-based detection and quarantine sensors/actuators for MANET systems.
FY 2008 Plans:
-- Research and develop techniques for authenticating and accounting for the use of all MANET resources.
-- Research and develop methods for denying all but authorized MANET traffic.
-- Research and develop methods for tolerating purposely induced failures from one or more MANET nodes and applications.
FY 2009 Plans:
-- Prototype and evaluate a combined assurable MANET infrastructure.
-- Research and prototype a secondary defensive system.

	FY 2007	FY 2008	FY 2009
Trustworthy Systems	4.408	12.800	10.000

(U) The goal of the Trustworthy Systems program is to provide foundational trustworthy computer platforms for Defense Department computing systems. This program seeks to develop technologies such as novel computer processing architectures, hardware, firmware, or microkernels to guarantee network and workstation security and will initially focus on network-based monitoring approaches that provide maximum coverage of the network with performance independent of the network size. These technologies will protect Defense systems from a wide-range of software problems, ranging from worms and Trojan horses, to bug-ridden software. This effort will focus on the development of feedback control-based solutions to software vulnerabilities and gateway-and-below network traffic monitoring approaches that scale with network size. The design of the controller component will leverage virtual machines to provide hardware-equivalent protection for the controller that specifically monitors the trustworthiness state of the application of interest, map the observations to a model of trustworthiness for that application, then decide what, if any, control actions need to be taken. Operational goals of the network-monitoring component include (1) improved probability of detection/probability of false alarm performance and (2) scalability to future gateway line speeds. The desired result is to allow software to be imperfect while mitigating catastrophic failures. Technical challenges include remotely monitoring mission-critical servers using

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

virtual machines, tracking the trustworthiness of the server, and controlling the server to return it to trustworthiness states. Primary end users identified to date include STRATCOM JTF/GNO and HQ PACOM. Transition partners include NCSC, NIWA, and DISA.

(U) Program Plans:

FY 2007 Accomplishments:

- Enabled the ability to detect and respond to next generation malicious software including stealthy "backdoors" to the operating system kernel (rootkits) and networks of compromised computers.
- Developed tools to find vulnerabilities in complex open source software.
- Surveyed state-of-art in virtual machine software technology.
- Evaluated capabilities of closed-feedback system for automated recovery of corrupted systems.

FY 2008 Plans:

- Develop scalable formal methods to verify complex hardware/software.
- Research network-sensitive approaches to monitor, and trustworthy controllers to control, how and when information is disseminated across the network based on network performance, load, criticality, and target capacity.
- Investigate the use of new virtual machine hardware architectures to develop a feedback loop that enables the host to monitor and control its behavior in the presence of untrustworthy software.
- Investigate secure hardware designs, software architectures, and code assessment technologies.
- Evaluate client-side controller software in laboratory environment.

FY 2009 Plans:

- Develop client-side laboratory-scale software and server-side virtual-machine based automated recovery.
- Harden and evaluate client-side controller code for field-deployable operations.
- Research network-sensitive approaches to monitor how and when information is disseminated across the network based on network performance, load, criticality, and target capacity.
- Develop high-throughput sensors, low-latency collection networks, and high-speed analyzers to assimilate the data.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

	FY 2007	FY 2008	FY 2009
DARPA Future Information Assurance Initiatives	3.878	8.250	0.000

(U) The DARPA Future Information Assurance Initiatives will identify promising technologies to enable remote command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) warfighting. Sophisticated computing capabilities currently available in desktop workstation and server systems are moving to mobile wireless embedded systems that communicate over low-bandwidth self-organizing tactical networks. As a result, the spectrum of devices the U.S. military must protect is increasing from wired and wireless tactical and garrison computers to include a wide array of small mobile devices. With foreign production of information technology components increasing and adversaries seeking to leverage cyber warfare as the Achilles' heel of current and future U.S. military systems; the U.S. military must have the ability to withstand, operate through, and counter increasingly effective cyber attacks while reducing the manpower required. Other distinct programs within this project will be created to pursue promising technologies as they are identified for further focused development. Included in this initiative is the development of secure, efficient network protocols to exploit tomorrows network-centric technologies such as networked weapons platforms, mobile ad-hoc networks, and end-to-end collaboration (vice client-server paradigm).

(U) Program Plans:

FY 2007 Accomplishments:

- Developed automatic techniques to modify computer applications to add information assurance properties (e.g. confidentiality, authentication, and others).
- Developed the ability to protect the core signaling and control of converged networks running voice over internet protocol (VOIP), wireless, voice, and data networks in enterprise telecommunications.
- Developed the ability to identify and authenticate hosts on the network and allow these hosts to discover their network's operating attributes.

FY 2008 Plans:

- Develop a family of distributed, autonomous security devices to deal with asymmetric traffic on wide area networks.
- Develop a secure, efficient network routing protocol for tomorrow's weapon, logistic, and command and control requirements.
- Develop a wireless protocol that securely provides location, authentication, and communications in a practical manner.
- Investigate new approaches to network security that scale with increased data rates and address spaces of future networks.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

	FY 2007	FY 2008	FY 2009
Control Plane	7.709	7.296	5.500

(U) The Control Plane program will improve end-to-end network performance between the Continental United States (CONUS) operating base and forward deployed tactical units. Control Plane seeks to develop the ability for individual hosts (end-points) to learn essential characteristics about the network, allowing the hosts to shape the network and network traffic to optimize network loading, prioritize traffic, and create communities of interest. Under Control Plane, when multiple network paths are available, hosts will be able to choose the best path/community or simultaneously transmit over multiple paths/communities. This technology will support the Defense Department's Global Information Grid concept of operations.

(U) Program Plans:

FY 2007 Accomplishments:

- Initiated development of hardware and software mechanisms to improve end-to-end wide-area network performance between the CONUS operating base and forward deployed tactical units.

FY 2008 Plans:

- Complete development of hardware and software mechanisms to improve end-to-end wide-area network performance between the CONUS operating base and forward deployed tactical units.
- Develop the ability of individual hosts (end-points) to learn essential characteristics about the network path between themselves and their transition partners through network query protocols.
- Investigate authentication protocols for secure transmission of network performance information.
- Develop the ability of hosts to learn about more than one possible transmission path, other hosts' abilities and purpose, and form communities of interest which suits their collective needs best.
- Develop the ability of hosts to simultaneously use multiple network paths for the same data transmission with the same partner, increasing communications speed and reliability.

FY 2009 Plans:

- Conduct demonstrations in operationally relevant environments.
- Demonstrate overall network transmission speed up to 60 Gbps using multiple fibers simultaneously.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

– Transition Control Plane technology to the Services.

	FY 2007	FY 2008	FY 2009
Wide Area Network (WAN) Monitoring	2.256	3.000	0.000

(U) The Wide Area Network (WAN) Monitoring effort seeks to develop distributed network monitoring capabilities and devices that can be used to identify, characterize, enable, optimize, visualize, and protect the WANs that compose the DoD enterprise Global Information Grid (GIG). This program will develop advanced capabilities to monitor the WANs that will comprise the GIG to detect malicious behavior, routing problems, or compromised mission capability. Goals include improved detection and false-alarm performance over conventional intrusion detection systems and scalability to the larger networks. This technology will support the DoD's GIG Information Assurance Technical Framework.

(U) Program Plans:

FY 2007 Accomplishments:

– Researched high-throughput hardware to implement the algorithms at the sensor layer.
– Investigated low-latency networks to collect the information.
– Investigated high-speed analyzers to assimilate the data and detect perturbations.

FY 2008 Plans:

– Investigate algorithms that quickly characterize various host's security configurations, identity, and classification as well as measure the type and quantity of information exchange.
– Analyze technologies to synthesize and visualize extremely large networks to improve leadership's situational awareness at the enterprise level.
– Research integrating and testing components in a fully functional configuration.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

	FY 2007	FY 2008	FY 2009
Spread Spectrum Networking	1.100	5.000	0.000

(U) Spread spectrum communication technology will significantly improve security against a variety of network attacks and identification profiles by spreading energy over a broad bandwidth, thereby providing an adversary with a signal which is both difficult to detect, as well as difficult to jam without using significant resources. This program is examining the potential of these same goals, by addressing not just the physical layer but also the entire network stack. Similar to frequency-hopping spread spectrum, the approach of this program studies algorithms that would provide hopping between Internet Protocol addresses and then expanding to hopping between different permutations of layer 1-3 protocols. The utility will provide significantly improved security against a variety of network attack and identification profiles.

(U) Program Plans:

FY 2007 Accomplishments:

- Modeled the problem of protecting wireless communications against cross-layer denial-of-service attacks with a game-theoretic approach.
- Demonstrated the performance of the spread spectrum networking approach for protection against smart attacks.

FY 2008 Plans:

- Investigate efficient smart-jammers against a communication system and developed countermeasures based on the Spread Spectrum approach.
- Document spread spectrum networking lessons learned.

	FY 2007	FY 2008	FY 2009
Control-Based Mobile Ad-Hoc Networks (CBMANET)	9.199	11.560	12.500

(U) The Control-Based Mobile Ad-Hoc Networks (CBMANET) program is developing an adaptive networking capability that dramatically improves performance and reduces life-threatening communication failures in complex communication networks. In order to develop this new capability, the initial focus is on tactical mobile ad-hoc networks (MANETs) that are inadequately supported with commercial technology.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

Conventional MANETs are composed of interdependent nodes based on interdependent system layers. Each MANET node exposes tens to hundreds of configurable parameters that must be continuously adapted due to variable tactical factors such as mission profile, phase, force structure, enemy activity, and environmental conditions. The complexity of this high-dimensional, adaptive, constrained, distributed network configuration problem is overwhelming to human operators and designers and has root causes in the historically wire-line-oriented networking paradigms. This program will take on the ambitious goal of researching a novel protocol stack that supports integrated optimization and control of all network layers simultaneously. Key technical challenges include scalable design, stability, and convergence. These challenges are particularly difficult in a distributed setting with partial and uncertain information, high communications overhead, and high probability of link failure. To address this problem, the CBMANET program will exploit recent optimization-theoretic breakthroughs, recent information-theoretic breakthroughs, and comprehensive cross-layer design to develop a network stack from first principles with specific attention to support for DoD applications such as multicast voice and situation awareness.

(U) Program Plans:

FY 2007 Accomplishments:

- Designed and prototyped two novel network protocol architectures based on information theory and optimization theory.
- Designed and analyzed protocols based on network coding that vastly improve performance in extreme conditions.
- Designed and analyzed cross-layer protocols and adaptive control capabilities to drive resource allocation more efficiently.
- Performed quantitative analysis and trade studies to understand the degree of performance offered by two novel network architectures.
- Researched requirements for a radio hardware platform to optimally support the novel network stacks.

FY 2008 Plans:

- Demonstrate and evaluate both technologies in realistic DoD scenarios using modeling and simulation.
- Design appropriate interfaces between the CBMANET network stacks and the physical radios in support of cross-layer optimization.
- Integrate the novel network architectures with physical radios in preparation for field demonstrations.

FY 2009 Plans:

- Undertake field demonstrations in challenging tactical environments.
- Research integrated coding and backpressure-based quality of service.
- Transition activities to the Services.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

	FY 2007	FY 2008	FY 2009
Security-Aware Systems	11.015	16.680	14.000

(U) The Security-Aware Systems program will develop and advance a variety of potentially promising technologies to enable the military to field secure, survivable, self-monitoring, self-defending network centric systems. Today's military software systems are brittle in the face of changing requirements. They are vulnerable to skilled attackers who develop creative and unpredictable strategies. Misconfiguration accounts for most security failures in Internet services and poses a serious risk to military systems. This program will develop security aware systems that will avoid brittleness and vulnerability, due to their ability to reason about their own security attributes, capabilities and functions with respect to specific mission needs. These systems will also dynamically adapt to provide desired levels of service while minimizing risk and providing coherent explanations of the relative safety of service level alternatives. These systems will bolster the reliability and security of critical open source software systems by reducing vulnerabilities and logic errors, and providing state-of-the-art software analysis techniques augmented with cognitive decision-making techniques with the ultimate goal of applying these systems on to the Global Information Grid. The Security-Aware Systems program consists of two efforts, Applications Communities (AC) and Self-Regenerative Systems (SRS).

- The Application Communities (AC) effort will develop technologies to protect DoD information systems that employ commercial software applications against cyber attack and system failure by developing collaboration-based defenses that detect, respond to, and heal with little or no human assistance. The effort will leverage advances in information assurance research programs to create a new generation of self-defending software that automatically responds to threats, and provides a comprehensive picture of security properties, displayed at multiple levels of abstraction and formality. This capability will bring intelligent security adaptation to DoD systems and make security properties and status more apparent to decision makers. AC technology will enable collections of similar systems to collaboratively generate a shared awareness of security vulnerabilities, vulnerability mitigation strategies, and early warnings of attack. AC will revolutionize the security of military information systems and reduce the threat from stealthy intrusion of critical systems and/or denial of service attacks.

- The Self-Regenerative Systems (SRS) effort will design, develop, demonstrate and validate architectures, tools, and techniques for fielding systems capable of adapting to novel threats, unanticipated workloads and evolving system configurations. SRS technology development of this effort will employ innovative techniques like biologically-inspired diversity, cognitive immunity and healing, granular and scalable redundancy, and higher-level functions such as reasoning, reflection and learning. SRS technologies will make critical future

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

information systems more robust, survivable and trustworthy. SRS will also develop technologies to mitigate the insider threat. SRS-enabled systems will be able to reconstitute their full functional and performance capabilities after experiencing accidental component failure, software error, or even an intentional cyber-attack. These systems will also show a positive trend in reliability, actually exceeding initial operation capability and approaching a theoretical optimal performance level over long periods while maintaining robustness and trustworthiness attributes.

(U) Research efforts will also explore workstation-class systems (including "trusted systems") which at present do not provide provable separation of information at different security levels, or provable protection of high-integrity applications from low-integrity applications. A new kind of computer workstation is needed whose architecture enables both formal proof and exhaustive validation of critical information and program separation properties (e.g., information in one graphical user interface (GUI) window never leaks to another GUI window).

(U) Program Plans:

FY 2007 Accomplishments:

- Developed an Application Community (AC) system architecture and demonstrated a working prototype that showed learning of program behavior that can be used to protect and repair software systems.

FY 2008 Plans:

- Develop techniques to collaboratively diagnose and respond to problems (e.g., attacks or failures that threaten a mission) in groups of military systems.
- Develop techniques to summarize security policy and status so the descriptions produced by AC can be understood without omitting critical details.
- Develop static and dynamic source code analysis techniques (e.g., data and control-flow-based techniques, model-checking, strong typing) to relate software module structures and runtime state with the representation of security properties/configurations.
- Demonstrate self-explanation techniques in which systems explain their critical security properties and status in a manner that is understandable to a variety of managing software components and human operators.
- Develop additional general strategies to automatically immunize systems against new attacks and preempt insider attacks; enabling anomaly detection, combining and correlating information from system layers, and using direct user challenges.

FY 2009 Plans:

- Develop, test and validate regimes to assess the protection mechanisms of security products, and certify protection to quantifiable levels based on a scientific rationale.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

- Develop measures to quantitatively characterize various dimensions of security (availability, integrity, confidentiality, authentication, and non-repudiation), fault tolerance, and intrusion tolerance, and demonstrate the theory's relevance by applying it to a realistic exemplar system.
- Tailor an exemplar self-regenerative system representative of a military application, thereby demonstrating the protective value to the warfighter.
- Conceptualize a new computer workstation architecture that enables both formal proof and exhaustive validation of critical information and program separation properties.
- Formulate a "trust hierarchy" rooted at user-visible peripheral devices (mouse, keyboard, speakers, and display) and extending down to traditional kernel mechanisms and applications.

	FY 2007	FY 2008	FY 2009
Quantum Key Distribution over Wide-Area Fiber Optic Networks	0.000	0.000	3.000

(U) The prevailing method for securing information transmitted across DoD and Intelligence networks is through the use of end-to-end encryption. This requires frequent secure distribution of encryption keys across the network. Quantum key distribution could offer this capability across the network, resulting in enhanced security from eavesdropping, code-breaking and spoofing. The program's objective is to develop an end-to-end quantum key distribution capability that works over a wide-area fiber-optic network. Today, this technology has been demonstrated only for point-to-point connections over distances of less than 200 kilometers. A key technical challenge is to extend the quantum key distribution capability to national, or global, dynamically switched fiber-optic networks. The needed advancements to enable this are the creation of a "quantum repeater" and the development of the associated key distribution protocol. The goal of the program is to demonstrate this capability experimentally over an existing DoD wide-area test network.

(U) Program Plans:

FY 2009 Plans:

- Complete an analysis of quantum encryption over classic fiber-optic networks.
- Develop candidate technologies and protocols for quantum key distribution over global-scale fiber-optic networks.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

	FY 2007	FY 2008	FY 2009
System for Planning Information Operations and Nonkinetic Effectiveness (SPINE)	0.000	0.000	3.417

(U) The System for Planning Information Operations and Nonkinetic Effectiveness (SPINE) program will improve operational effectiveness, operational tempo, tool performance, tool development, decrease training requirements, enable scalable operations not possible today, and demonstrate the full potential of Information Operations (IO) capabilities due to their newly quantified performance metrics. The significant challenge is the development of models for non-kinetic weapons that are comparable to today's physics-based kinetic models. Those models are critical to demonstrating the effectiveness of non-kinetic weapons and configuring an IO range capable of collecting the diverse empirical data required to provide confidence in the measurements. The program will develop the following: first, measurement techniques to quantify the effectiveness of IO weapons; second, a planning system to give the combatant commander the ability to determine which combination of kinetic or non-kinetic weapons they should use during operations.

(U) Program Plans:
FY 2009 Plans:
- Develop algorithms/software to provide quantified metrics on Computer Network Attack tool performance.
- Expand tool suite to measure anticipated weapon performance based on known & estimated target network characteristics.
- Develop planning system that can select optimal course of action based on marriage of target configuration intelligence and quantified tool characteristics.

	FY 2007	FY 2008	FY 2009
Rootkit Detection	0.000	0.000	3.500

(U) Based on results from the Future Information Assurance program, Rootkit Detection will assess the current and emerging state-of-the-art rootkit (software tools intended to conceal running processes, files or system data from the operating system) technology, detection and mitigation in the context of the DoD and leverage experience with rootkits and detection and mitigation methods. After collecting rootkits and detection tools and methods, this program will establish knowledge of future rootkit trends and detection mechanisms. Technical goals include identifying trends

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

in rootkit developments, anticipating next generation threats, and developing advanced detection and mitigation techniques. Possible approaches include: detection of indirect effects of rootkits (not implementation-specific effects), creation of abnormal usage conditions on the system to induce indirect effects, collection of evidence from multiple perspectives, and use of Bayesian Networks to reason over evidence. Comprehensive, objective and empirical data regarding the threat posed by rootkits, how well current approaches address that threat, characteristics and metrics for each approach and identification of (1) promising detection approaches and (2) key gaps. This program will address the growing threat of rootkits to DoD IT systems and networks.

(U) Program Plans:

FY 2009 Plans:

- Design and implement laboratory-scale automated rootkit detection and mitigation software.
- Evaluate developed software in laboratory environment.
- Harden laboratory-level code into field-deployable rootkit detection and mitigation system.
- Evaluate developed system in military information operations range.

	FY 2007	FY 2008	FY 2009
Defensive Autonomous Systems	0.000	0.000	3.000

(U) The Defense Autonomous Systems goal is to allow the military to more closely monitor and identify remotely-controlled computers (bots) and bot slaves within military and government networks, as well as increase the monitoring capability of our defenders. This program will develop novel software to enable this capability. Utilizing the border gateway protocol, this program will provide policy based routing between large pieces (i.e., autonomous systems) of the Internet. By building concentric rings from autonomous systems, it is possible to hide all or part of a network from people outside of the rings (e.g. on the Internet). By monitoring the interconnection points between the outer and inner ring, it is possible to identify all bot slaves and controllers because bot command and control traffic is fairly regular and has a unique signature. In order to monitor and mitigate against attacks from bot networks we must automate the tools we currently use. Adding the additional autonomous systems to existing military networks requires the military Services to request the new autonomous system, properly design and configure the interconnection, and monitor the system to detect an attack within minutes.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

(U) Program Plans:
FY 2009 Plans:
- Identify specific bot signatures and their uniqueness.
- Develop prototype mechanisms to test and evaluate this technique on military data networks.
- Design and implement laboratory-level automated detection, reverse engineering, and mitigation system.
- Modify existing router filters to identify bot traffic (or develop high-speed network devices if necessary).
- Develop a database for the routers (or the high-speed devices) to communicate with, storing the address and identity of bots and bot controllers.

	FY 2007	FY 2008	FY 2009
Software Assurance Education and Research	0.000	1.000	0.000

(U) Program Plans:
FY 2008 Plans:
- Conduct research in software assurance education.

	FY 2007	FY 2008	FY 2009
National Repository of Digital Forensic Intelligence	0.000	1.120	0.000

(U) This effort will focus on the goal of the National Repository of Digital Forensic Intelligence.

(U) Program Plans:
FY 2008 Plans:
- Pursue efforts relating to the National Repository of Digital Forensic Intelligence.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

(U) Other Program Funding Summary Cost:

- Not Applicable.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)						DATE February 2008	
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research			R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-04				
COST (In Millions)	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Language Translation IT-04	70.539	71.423	75.019	72.433	52.593	52.593	52.593

(U) Mission Description:

(U) This project is developing powerful new technologies for processing foreign languages that will provide critical capabilities for a wide range of military and national security needs, both tactical and strategic. The technologies and systems developed in this project will enable our military to automatically translate and exploit large volumes of speech and text in multiple languages obtained through a variety of means.

(U) Current U.S. military operations involve close contact with a wide range of cultures and peoples. The warfighter on the ground needs hand-held, speech-to-speech translation systems that enable communication with the local population during tactical missions. Thus tactical applications imply the need for two-way (foreign-language-to-English and English-to-foreign-language) translation.

(U) Because foreign-language news broadcasts, web-posted content, and captured foreign-language hard-copy documents can provide insights regarding local and regional events, attitudes and activities, language translation systems also contribute to the development of good strategic intelligence. Such applications require one-way (foreign-language-to-English) translation. Exploitation of the resulting translated content requires the capability to automatically collate, filter, synthesize, summarize, and present relevant information in timely and relevant forms.

(U) Program Accomplishments/Planned Programs:

	FY 2007	FY 2008	FY 2009
Spoken Language Communication and Translation System for Tactical Use*	16.757	14.188	11.533

*Formerly known as Situation Presentation and Interaction.

(U) The Spoken Language Communication and Translation System for Tactical Use (TRANSTAC) program will develop technologies that enable robust spontaneous two-way tactical speech communications between our warfighters and native speakers. The program addresses the issues surrounding the rapid deployment of new languages, especially, low-resource languages and dialects. TRANSTAC is building upon

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-04

existing speech translation platforms to create a rapidly deployable language tool that will meet the military's language translation needs. TRANSTAC is currently focusing on key languages of the Middle East region.

(U) Program Plans:

FY 2007 Accomplishments:

- Performed mission needs analysis and aggressive initial language data collection.
- Demonstrated a proof-of-principle, two-way Iraqi Arabic system free-form exchange between English and Iraqi Arabic speakers in specific domains.
- Provided seventy-five (75) Iraqi Arabic Systems for in-theater experimental fielding.
- Established a Call-A-Translator Service in Iraq for in-field use and rapid data collection.
- Demonstrated prototype two-way Farsi system.

FY 2008 Plans:

- Perform additional mission needs analysis and aggressive language data collection.
- Develop new two-way translation software technologies for insertion into, and enhancement of, the two-way Iraqi systems.
- Develop tools for rapid deployment of new languages and dialects.
- Further enhance recognition and translation performance.
- Develop smaller form-factor prototypes to facilitate mobile use (towards eyes-free, hands-free) translation systems.
- Increase robustness of the prototypes to address the issue of noisy environments.

FY 2009 Plans:

- Update/enhance the experimental systems in the field.
- Continue mission needs analysis and aggressive language data collection.
- Develop two-way translation systems in other languages that will enable the user to not only translate words but also communicate and carry on limited conversation.
- Develop context management translation techniques.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-04

	FY 2007	FY 2008	FY 2009
Global Autonomous Language Exploitation (GALE)*	50.654	48.935	46.396

*Formerly part of Automated Speech and Text Exploitation in Multiple Languages.

(U) The Global Autonomous Language Exploitation (GALE) program will develop and integrate technology to enable automated transcription and translation of foreign speech and text along with content summarization. Presently, the exploitation of foreign language speech and text is slow and labor intensive. GALE will provide, in an integrated product, automated transcription and translation of foreign speech and text along with content summarization. When applied to foreign language broadcast media and web-posted content, GALE will enhance open-source intelligence and local/regional situational awareness and eliminate the need for translation and subject matter experts at every military site where such information is obtained. Thus, GALE will also reduce the military manpower requirements for translators and mitigate the escalating need for trained support personnel. GALE will tightly integrate multidisciplinary research and produce prototype systems. Earlier DARPA work in foreign language processing yielded an initial integrated architecture concept for speech transcription and text translation, resulting in near edit-worthy text. Continuing work under GALE will produce a fully mature integrated architecture and dramatically improve transcription and translation accuracy by exploiting context and other clues. GALE will address unstructured speech such as talk show conversations and chat room communications and develop timely, succinct reports and alerts for commanders and warfighters.

(U) Program Plans:

FY 2007 Accomplishments:

- Designed and documented a GALE architecture based on the industry standard Unstructured Information Management Architecture (UIMA).
- Created architectural components that combine the output of multiple machine translation engines.
- Identified workflows of all processing engines and provided integration of these workflows on top of the architectural foundation.
- Developed an integrated approach where the problem is viewed mathematically as a single system, with foreign speech/text as input, and English text and distilled information as output.
- Evaluated GALE translation engines on Arabic and Chinese languages for structured and unstructured speech and text.
- Improved translation capabilities, reducing the translation errors by a factor of two in the first year.
- Evaluated summarization technologies.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-04

– Performed a utility study and evaluated the effectiveness of the end-to-end system relative to a baseline search engine.

FY 2008 Plans:

– Develop methods to optimize the parameters of speech-to-text acoustic models such that transcription errors are minimized on the training data.
– Develop discriminative training algorithms to optimize word alignment and translation quality.
– Implement an integrated search of speech-to-text transcription and machine translation.
– Integrate metadata extraction into the speech-to-text components.
– Evaluate translation and summarization technologies.
– Transition technologies developed by the GALE program into high-impact military systems and intelligence operations centers.
– Incorporate syntax analysis with machine translation algorithms.

FY 2009 Plans:

– Develop methods for porting technology into new languages.
– Perform design and feasibility experiments for extraction-empowered machine translation, where the system extracts the meaningful phrases (e.g., names and descriptions) from foreign language text for highly accurate translation into English.
– Incorporate predicate-argument analysis to enhance machine translation and summarization.
– Complete the architecture for a summarization system that incorporates adaptive filtering, focused summarization, information extraction, contradiction detection, and user modeling.

	FY 2007	FY 2008	FY 2009
Multilingual Automatic Document Classification, Analysis and Translation*	3.128	8.300	12.414

*Formerly part of Automated Speech and Text Exploitation in Multiple Languages.

(U) The Multilingual Automatic Document Classification, Analysis and Translation (MADCAT) program will develop and integrate technology to enable exploitation of captured, foreign language, hard-copy documents. Hard-copy documents, including notebooks, letters, ledgers, annotated maps, newspapers, newsletters, leaflets, pictures of graffiti, and document images (e.g., PDF files, JPEG files, scanned TIFF images, etc.) resident on magnetic and optical media captured in the field may contain important but perishable information of great potential value to the warfighter. These documents often contain machine printed and handwritten text in various combinations and orientations in one or

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-04

more languages. Unfortunately, due to limited human resources and the immature state of applicable technology, our military does not currently have the ability to exploit, in a timely fashion, ideographic and script documents that are either machine printed or handwritten in Arabic or Chinese. The MADCAT program will address this need by producing devices that would enable soldiers to convert such captured documents to readable English in the field. MADCAT will substantially improve the applicable technologies, in particular document analysis and optical character recognition/optical handwriting recognition (OCR/OHR), tightly integrate these with translation technology, and create technology demonstration prototypes for field trials.

(U) Program Plans:

FY 2007 Accomplishments:

- Implemented new methods for Optical Character Recognition using 2-D linear transform techniques and graph theory matching techniques.

FY 2008 Plans:

- Improve methods for document segmentation (e.g., title, address box, columns, lists, embedded picture/diagram/caption, annotation, signature block, etc.).
- Improve script (e.g., Roman vs. Cyrillic) and language (e.g., Farsi vs. Arabic) identification.
- Develop algorithms for document type identification (e.g., letter, ledger, annotated map, newspaper, etc.).
- Develop means to discriminate and separate handwriting from printed regions and improve OCR/OHR technologies.
- Develop the means to interpret different regions within a document, for example, to extract the particulars from an address field or the axes of a table.

FY 2009 Plans:

- Develop algorithms to predict the syntactic structure and propositional content of text.
- Develop tightly integrated technology prototypes that convert captured documents into readable and searchable English.
- Integrate these improvements with the translation and summarization components of GALE.
- Enable efficient metadata-based search and retrieval.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-04

	FY 2007	FY 2008	FY 2009
Robust Automatic Translation of Speech (RATS)	0.000	0.000	4.676

(U) The Robust Automatic Translation of Speech (RATS) program will address noisy and hostile conditions where speech is degraded by distortion, reverberation, and competing conversations. Research into the issue of robustness to enhance the capabilities of speech processing would enable soldiers to hear or read clear English versions of what is being said in their vicinity, despite the noisy environment. RATS technology will build upon advances in GALE technology.

(U) Program Plans:
FY 2009 Plans:
- Improve the robustness of automatic speech transcription and translation algorithms in adverse environments (noise, distortion, reverberation, and competing speech signals).
- Evaluate the relative benefits (performance versus computational requirements) of noise suppression and speech exploitation based on a single microphone versus using multi-microphone arrays.
- Assess the utility of eye-tracking as an adjunct to audio-based source localization.

(U) Other Program Funding Summary Cost:

- Not Applicable.