Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Army										DATE: February 2012	
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*				R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*							
COST ($ in Millions)	**FY 2011**	**FY 2012**	**FY 2013 Base**	**FY 2013 OCO**	**FY 2013 Total**	**FY 2014**	**FY 2015**	**FY 2016**	**FY 2017**	**Cost To Complete**	**Total Cost**
Total Program Element	25.367	26.117	18.090	-	18.090	16.934	19.180	22.863	22.932	Continuing	Continuing
976: *ARMY THREAT SIM (ATS)*	25.367	26.117	18.090	-	18.090	16.934	19.180	22.863	22.932	Continuing	Continuing

Note

FY11 includes a Congressional Add of $9,166K for the JFCOM Mission Transfer.

A. Mission Description and Budget Item Justification

This program supports the design, development, acquisition, integration and fielding of realistic mobile threat simulators and realistic threat simulation products utilized in Army training and developmental and operational tests. While this project originally funded simulators representing Soviet equipment, the changing world order has expanded the scope of this program to address other world threats. Army Threat Simulator and Threat Simulation products are utilized to populate test battlefields for U.S. Army Test and Evaluation Command (ATEC), to conduct developmental and operational tests, and to support Program Executive Office (PEO) required user testing in System Integration Laboratories and hardware/simulation in-the-loop facilities. Army threat simulator and threat simulation products developed or fielded under this program support Army-wide, non-system specific threat product requirements. Each capability is pursued in concert and coordination with existing Army and tri-service capabilities to eliminate duplication of products and services, while providing the proper mix of resources needed to support Army testing and training. These battlefield simulators represent systems (e.g. missile systems, command, control and communications systems, electronic warfare systems, etc.) that are used to portray a realistic threat environment during testing of U.S. weapon systems. Simulator development is responsive to Office of the Secretary of Defense and General Accounting Office guidance for the Army to conduct operational testing in a realistic threat environment. Actual threat equipment is acquired when appropriate (in lieu of development) and total package fielding is still required (i.e., instrumentation, operations and maintenance, manuals, new equipment training, etc.). Threat simulator development is accomplished under the auspices of the Project Manager for Instrumentation, Targets and Threat Simulators (PM ITTS) and the Director, Operational Test and Evaluation, Threat Simulator Investment Working Group.

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Army					DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*				
B. Program Change Summary ($ in Millions)	**FY 2011**	**FY 2012**	**FY 2013 Base**	**FY 2013 OCO**	**FY 2013 Total**
Previous President's Budget	26.158	16.992	17.442	-	17.442
Current President's Budget	25.367	26.117	18.090	-	18.090
Total Adjustments	-0.791	9.125	0.648	-	0.648
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	9.166			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.519	-			
• Adjustments to Budget Years	-	-	0.648	-	0.648
• Other Adjustments 1	-0.272	-0.041	-	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2013 Army			DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*	

COST ($ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
976: *ARMY THREAT SIM (ATS)*	25.367	26.117	18.090	-	18.090	16.934	19.180	22.863	22.932	Continuing	Continuing
Quantity of RDT&E Articles											

A. Mission Description and Budget Item Justification

This program supports the design, development, acquisition, integration, and fielding of realistic mobile threat simulators and realistic threat simulation products used in Army training, developmental tests, and operational tests. While this project originally funded simulators representing Soviet equipment, the operational environment has expanded the scope of this program to address other world threats. Army Threat Simulator and Threat Simulation products are used to populate test battlefields for U.S. Army Test and Evaluation Command (ATEC), to conduct developmental and operational tests, and to support Program Executive Office (PEO) required user testing in System Integration Laboratories and hardware/simulation in-the-loop facilities. Army threat simulator and threat simulation products developed or fielded under this program support Army-wide, non-system specific threat product requirements. Each capability is pursued in concert and coordination with existing Army and tri-service capabilities to eliminate duplication of products and services, while providing the proper mix of resources needed to support Army testing and training. These battlefield simulators represent systems (e.g. missile systems, command, control and communications systems, electronic warfare systems, etc.) that are used to portray a realistic threat environment during testing of U.S. weapon systems. Simulator development is responsive to Office of the Secretary of Defense and Government Accountability Office guidance for the Army to conduct operational testing in a realistic threat environment. Actual threat equipment is acquired when appropriate (in lieu of development) and total package fielding is still required (i.e., instrumentation, operations and maintenance, manuals, new equipment training, etc.). Threat simulator development is accomplished under the auspices of the Project Manager for Instrumentation, Targets and Threat Simulators (PM ITTS) and the Director, Operational Test and Evaluation, Threat Simulator Investment Working Group.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2011	FY 2012	FY 2013
Title: Continues Engineering Manfacturing and Development (EMD) for the Network Exploitation Test Tool (NETT).	3.253	3.332	3.461
Articles:	0	0	
Description: Continues EMD for the NETT as a comprehensive Computer Network Operations (CNO) tool.			
FY 2011 Accomplishments: Continued EMD for the Network Exploitation Test Tool (NETT) as a comprehensive Computer Network Operations (CNO) tool, designed for Test & Evaluation (T&E), to portray evolving hostile and malicious Threat effects within the cyber domain. The program provided an integrated suite of open-source/open-method exploitation tools which were integrated with robust reporting and instrumentation capabilities. NETT was used by Threat CNO teams to replicate the tactics of state and non-state Threat and was supported by a robust CNO development environment and has steadily incorporated leading Threat tools, tactics, techniques, and procedures.			
FY 2012 Plans:			

Exhibit R-2A, RDT&E Project Justification: PB 2013 Army		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2011	FY 2012	FY 2013
Continues EMD for the Network Exploitation Test Tool (NETT). Network Exploitation Test Tool is a comprehensive Computer Network Operations (CNO) tool, designed for T&E, to portray evolving hostile and malicious Threat effects within the cyber domain. The program provides an integrated suite of open-source/open-method exploitation tools which are integrated with robust reporting and instrumentation capabilities. NETT is used by Threat CNO teams to replicate the tactics of state and non-state Threat and is supported by a robust CNO development environment. Current hacking tools and capabilities are being introduced daily to the hacking community. The NETT program researches these new capabilities and uses an in-depth process to clean, fix, and integrate required Threat tools, tactics, and techniques that are needed during T&E. ***FY 2013 Plans:*** NETT is a comprehensive Computer Network Operations (CNO) tool, designed for T&E, to portray evolving hostile and malicious Threat effects within the cyber domain. The program will provide an integrated suite of open-source/open-method exploitation tools which are integrated with robust reporting and instrumentation capabilities. NETT will be used by Threat CNO teams to replicate the tactics of state and non-state Threat and will be supported by a robust CNO development environment. Current hacking tools and capabilities will be introduced daily to hacking community. The NETT program researches these new capabilities and utilizes an in-depth process to clean, fix, and integrate required Threat tools, tactics, and techniques that are needed during T&E. FY13 funding will support the continuation of exploit development, will continue support to the NETT Users Group, and will maintain pace with advanced exploit research and tool integration required to support the growing demand for the Threat CNO Team and mission.			
Title: Congressional Add - Threat Simulator Development Unfunded Joint Forces Command (JFCOM) Mission Transfer. ***Articles:*** ***Description:*** Completes the engineering and manufacturing Development (EMD) for Joint Forces Command (JFCOM) Mission Transfer. ***FY 2012 Plans:*** Completes the Engineering and Manufacturing Development (EMD) required to facilitate the seamless Joint Forces Command (JFCOM) Mission Transfer.	-	9.166 0	-
Title: Government Program Management for the Threat Systems Management Office Operations (TSMO). ***Articles:*** ***Description:*** Government Program Management for TSMO. ***FY 2011 Accomplishments:*** The Government Program Management for the Threat Systems Management Office Operations funded the maintenance management, and sustainment capability for Threat systems within the Army's Threat inventory. Satisfied the requirement to	2.660 0	2.904 0	2.704

Exhibit R-2A, RDT&E Project Justification: PB 2013 Army		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2011	FY 2012	FY 2013
provide operations and maintenance, spares, training, special tools, recurring Department of Defense Information Assurance and Certification Process (DIACAP), etc, for fielded Threat systems and infrastructure. Funding supported manpower, storage, and integration facilities associated with the sustainment and operational readiness of the Army's Threat force. ***FY 2012 Plans:*** Government Program Management for the TSMO Operations funds the maintenance management, and sustainment capability for Threat systems within the Army's Threat inventory. Funding supports manpower, storage, and integration facilities associated with the sustainment and operational readiness of the Army's Threat force. Satisfies the requirement to provide operations and maintenance, spares, training, special tools, recurring DIACAP, etc, for fielded Threat systems and infrastructure. ***FY 2013 Plans:*** Government Program Management for the TSMO Operations will fund the operation, maintenance, management, and sustainment capability for Threat systems used to portray a realistic threat environment during Army testing and training within the Army's Threat inventory. Will include acquisition life cycle management support (operation, maintenance, spares, new equipment training, special tools and instrumentation, safety, environmental, security, information assurance, etc) of new threat systems fielded into the Army's Threat inventory. Funding will support the scheduled entry and drawdown of equipment within the Threat inventory.			
Title: Continues Engineering and Manufacturing Development (EMD) for the Threat Intelligence and Electronic Warfare Environment (TIEW ENV). ***Articles:*** ***Description:*** Continues EMD for the Threat Intelligence and Electronic Warfare Environment (TIEW ENV) to simulate Electronic Warfare capabilities. ***FY 2011 Accomplishments:*** Continued EMD for the TIEW ENV that provided the constructive Threat representation environment for Army T&E and provided the primary capability to interact between live, virtual, and constructive Threat Information Operations (IO) environments. ***FY 2012 Plans:*** Continues EMD for the TIEW ENV. TIEW ENV provides the constructive Threat representation environment for Army T&E and provides the primary capability to interact between live, virtual, and constructive Threat IO environments. The TIEW ENV integrates Threat IO (Electronic Attack, Electronic Support, CNO) models into the One Semi-Automated Force (OneSAF) baseline. The models' representative effects are also integrated through use with Communications Effects Servers. Integration of OneSAF with the Integrated Threat Force (ITF) enables the Live and Constructive T&E environments to interface. ***FY 2013 Plans:***	3.874 0	4.027 0	3.967

Exhibit R-2A, RDT&E Project Justification: PB 2013 Army		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2011	FY 2012	FY 2013
Will continue EMD for the TIEW ENV. The TIEW ENV will support the establishment of a wrap-around threat environment required to evaluate, demonstrate, and employ the EW capabilities of Enemy Forces in simulated real-world test/training events. The TIEW ENV will provide the capability to import vignettes, establish virtual entities, connect live assets, and interact between the live, virtual, and constructive environments. The TIEW ENV will fully integrate with the ITF to enable Opposing Forces (OPFOR) command of threat EW assets across Live, Virtual, and Constructive (LVC) domains. FY13 will satisfy Army requirements by funding development, platform integration and sustainment of this capability. Program will field incremental capabilities in support of upcoming spin out events.			
Title: Continues the Engineering and Manufacturing Development (EMD) for the Integrated Threat Force (ITF), formerly named Threat Battle Command Center (TBCC) to support new threat systems/equipment. ***Articles:*** ***Description:*** Continues the EMD for the ITF to support new threat systems/equipment. ***FY 2011 Accomplishments:*** Continued the EMD for the ITF that provided an integrated, scalable Threat command and control for all Army Threat representations as well as provided the Test & Evaluation (T&E) solution to satisfy the System of Systems (SoS) requirement of a Free Thinking Threat force. ***FY 2012 Plans:*** Continues EMD for the ITF which provides an integrated, scalable Threat command and control for all Army Threat representations to provide the T&E solution to satisfy the SoS requirement of a Free Thinking Threat force. ***FY 2013 Plans:*** Will continues EMD for the ITF which will provide an integrated, scalable Threat command and control for all Army Threat representations. This program will leverage prior Central Test & Evaluation Investment Program (CTEIP) investments to create a highly adaptable and unique threat force capability required to meet T&E requirements for the evaluation of network-centric platforms and SoS capabilities by closely simulating expected real-world threat environments. FY13 funding will be used for the continued hardware/software development/build-out supporting the threat force architecture, visualization, Command and Control (C2), and fusion needs required to successfully meet scalability and reconfigurability needs for current T&E requirements.	3.858 0	3.899 0	4.510
Title: Continues the Engineering and Manufacturing Development (EMD) for the Threat Signal Injection Jammer (TSIJ). ***Articles:*** ***Description:*** Continues the EMD for the TSIJ to provide the Army an alternative to open-air Electronic Attack (EA) in a test environment. ***FY 2011 Accomplishments:***	1.128 0	0.411 0	-

Exhibit R-2A, RDT&E Project Justification: PB 2013 Army		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2011	FY 2012	FY 2013
Continued the EMD for the TSIJ to provide the Army an alternative to open-air Electronic Attack (EA) in a test environment by using direct input to a receiver unit and remote control on/off employment. ***FY 2012 Plans:*** Completes EMD for the TSIJ to provide the Army an alternative to open-air Electronic Attack (EA) in a test environment by using direct input to a receiver unit and remote control on/off employment. Develop design for 2-channel man-pack Remote Jamming Unit (RJU) and 10 watt environmentally sealed Control Signal Transmitter (CST) for TSIJ.			
Title: Completed the Engineering and Manufacturing Development (EMD) for the Control of Signal Transmission-Open Air Capability (CST-OAC) and Signal Intelligence/Direct Finding (SIGINT/DF). ***Articles:*** ***Description:*** Completed the EMD for the CST-OAC and SIGINT/DF sensors onto a larger aerial platform for Threat Devices capability. ***FY 2011 Accomplishments:*** Completed EMD for the CST-OAC and SIGINT/DF sensors onto a larger aerial platform for Threat Devices capability.	0.667 0	-	-
Title: Army Technical Test Instrumentation and Targets Project 62C Modeling and Simulation Instrumentation ***Articles:*** ***Description:*** Project 976 includes $7.600 million FY11 RDTE incorrectly placed in this funding line. ***FY 2011 Accomplishments:*** Project 976 includes $7.600 million FY11 RDTE incorrectly placed in this funding line. It was intended for 0605602A - Army Technical Test Instrumentation and Targets Project 62C Modeling and Simulation Instrumentation in support of operational and developmental testing.	7.600 0	-	-
Title: Continues Government Program Management for the Threat Computer Network Operations Teams (TCNOT) to support threat events. ***Articles:*** ***Description:*** Continues Government Program Management for the TCNOT to support threat events in order to maintain a team of highly qualified, trained, and certified Computer Network Operations (CNO) professionals qualified for the employment of Threat CNO in support of Army T&E. ***FY 2011 Accomplishments:***	2.327 0	2.378 0	3.448

Exhibit R-2A, RDT&E Project Justification: PB 2013 Army		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2011	FY 2012	FY 2013
Continued Government Program Management for the Threat Computer Network Operations Teams (TCNOT) to support threat events in order to maintain a team of highly qualified, trained, and certified CNO professionals qualified for the employment of Threat CNO in support of Army T&E. The mission was for the Threat CNO Team to accurately replicate the hacker intent of state and non-state Threats through identification of system vulnerabilities that could be exploited by Threat forces, replicating loss of service, or exploiting network enabled systems to gain critical information or create a desired effect. ***FY 2012 Plans:*** Continues EMD for the Threat CNO Team program. Threat CNO Team program establishes and maintains a team of highly trained and certified CNO professionals qualified for the employment of Threat CNO in support of Army T&E. The Threat CNO Team mission is to accurately replicate the hacker intent of state and non-state Threats through identification of system vulnerabilities that could be exploited by Threat forces, replicating loss of service, or exploiting network enabled systems to gain critical information or create a desired effect. ***FY 2013 Plans:*** Will continue EMD for the Threat CNO Team program. The Threat CNO Team program will establish and maintain a team of highly trained and certified CNO professionals qualified for the employment of Threat CNO in support of Army T&E. The Threat CNO Team mission is to accurately replicate the capabilities and hacker intent of state and non-state Threats through identification of Army system vulnerabilities that could be exploited by Threat forces, replicating loss of service, or exploiting network enabled systems to gain critical information or create a desired effect. The funding supports unique training, credentials, and authorizations involving organizations such as Army 1st IO Command, NSA, HQDA-G2, and industry. The FY13 will fund requirements to include continued research of the intelligence-based TCNO TTPs and threat portrayal capabilities up to the Nation State level; development of the necessary, highly specialized TCNO Training program; development, research, and analysis of continually emerging foreign threat capabilities; and data collection capability. The program will establish analytical services needed to identify and correlate data of historical and real time malicious activity within the Army Land Warrior Network (LWN) and external to the DOD. This program will also establish services and near real-time processing of information needed to develop threat targeting packages that accurately profile the cyber enemy, types of systems they attack, frequency of attacks, their intent, doctrine, training, techniques, tools and operational tactics. The program will result in creation of teams of Threat CNO professionals, working in concert with the Intelligence Community, capable of accurately portraying validated real world CNO threat to meet operational test requirements.			
Accomplishments/Planned Programs Subtotals	25.367	26.117	18.090

C. Other Program Funding Summary ($ in Millions)

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2013 Army		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

D. Acquisition Strategy

THREAT SIMULATOR Test Programs Supported: Aircraft (MH-47E) Follow On Operational Test II, MH-60K Aircraft, Aircraft (MH-60K) Follow On Operational Test II, RAH-66 Comanche EUTE, RAH-66 Comanche FDTE I, Suite of Integrated Radio Countermeasures (SIRFCM), Suite of Integrated Radio Countermeasures (SIIRCM), Unmanned Aerial Vehicle (UAV) - Payload, Force XXI Battle Command Brigade and Below, Army Airborne Command and Control, Army TACMS Block II/BAT, Bradley Fighting Vehicle-A3, Crusader FDTE, Extended Range MLRS, FAAD Block III, GPS in Joint Battle Space Environment, Guardrail/Common Sensor System II, Handheld Standoff Mine Field Detection System, IEW Tactical Proficiency Trainer, Joint Close Air Support HT&E, Joint Suppression of Enemy Air Defense (JSEAD), Land Warrior, Long Range Advanced Scout Surveillance System, Navigational Warfare Global Positioning System, OH-58D Kiowa Warrior, Patriot Advanced Capabilities PAC-3 Config-3, UH-60Q, Theater High Altitude Area Defense System.

E. Performance Metrics

Performance metrics used in the preparation of this justification material may be found in the FY 2010 Army Performance Budget Justification Book, dated May 2010.