

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2016 Army	Date: February 2015
---	----------------------------

Appropriation/Budget Activity 2040: Research, Development, Test & Evaluation, Army / BA 6: RDT&E Management Support	R-1 Program Element (Number/Name) PE 0604256A / Threat Simulator Development
---	--

COST (\$ in Millions)	Prior Years	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
Total Program Element	-	23.598	22.057	20.035	-	20.035	23.509	21.366	22.321	23.048	-	-
976: Army Threat Sim (ATS)	-	23.598	22.057	20.035	-	20.035	23.509	21.366	22.321	23.048	-	-

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. Project originally funded simulators representing Soviet equipment, but scope was expanded to address emerging 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.

B. Program Change Summary (\$ in Millions)	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total
Previous President's Budget	23.921	18.062	18.780	-	18.780
Current President's Budget	23.598	22.057	20.035	-	20.035
Total Adjustments	-0.323	3.995	1.255	-	1.255
• Congressional General Reductions	-	-0.005			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	4.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-0.043	-			
• SBIR/STTR Transfer	-0.280	-			
• Adjustments to Budget Years	-	-	1.255	-	1.255

Congressional Add Details (\$ in Millions, and Includes General Reductions)

Project: 976: Army Threat Sim (ATS)

FY 2014	FY 2015

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2016 Army		Date: February 2015	
Appropriation/Budget Activity 2040: <i>Research, Development, Test & Evaluation, Army / BA 6: RDT&E Management Support</i>		R-1 Program Element (Number/Name) PE 0604256A / <i>Threat Simulator Development</i>	
Congressional Add Details (\$ in Millions, and Includes General Reductions) Congressional Add: <i>Integrated Threat Distributed Cyber Environments</i>		FY 2014	FY 2015
		-	4.000
Congressional Add Subtotals for Project: 976		-	4.000
Congressional Add Totals for all Projects		-	4.000

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army										Date: February 2015		
Appropriation/Budget Activity 2040 / 6					R-1 Program Element (Number/Name) PE 0604256A / Threat Simulator Development				Project (Number/Name) 976 / Army Threat Sim (ATS)			
COST (\$ in Millions)	Prior Years	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
976: Army Threat Sim (ATS)	-	23.598	22.057	20.035	-	20.035	23.509	21.366	22.321	23.048	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		
Note												
Advanced Network Electronic Support Threat Sensors (NESTS), Advanced Jammer Suite (Next Generation Electronic Attack (EA) and Threat Information Environment are new starts in FY16. Threat Intelligence and Electronic Warfare Environment (TIEW ENV) ends in FY15.												
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. Project originally funded simulators representing Soviet equipment, but scope was expanded to address emerging 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.												
B. Accomplishments/Planned Programs (\$ in Millions)									FY 2014	FY 2015	FY 2016	
Title: Network Exploitation Test Tool (NETT).									10.257	3.776	3.788	
Description: Continues Engineering Manufacturing and Development (EMD) for the NETT as a comprehensive Computer Network Operations (CNO) tool.												
FY 2014 Accomplishments: Continued EMD for the NETT. NETT is a comprehensive Computer Network Operations (CNO) tool, designed for Test and 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 was 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. The Cyber domain is the most rapidly changing domain in which our systems operate.												

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015	
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0604256A / <i>Threat Simulator Development</i>	Project (Number/Name) 976 / <i>Army Threat Sim (ATS)</i>	
B. Accomplishments/Planned Programs (\$ in Millions)		FY 2014	FY 2015
<p>The NETT program researched these new capabilities and used an in-depth process to clean, fix, and integrate required Threat tools, tactics, and techniques that will be needed during T&E. Focus areas include continued Threat integration, instrumentation, distributed collaboration, and remote agent development.</p> <p>FY 2015 Plans: Continues EMD for the NETT. NETT will be 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 will be 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 will be supported by a robust CNO development environment. The Cyber domain will be the most rapidly changing domain in which our systems operate. 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. Focus areas include continued Threat integration, instrumentation, distributed collaboration, and remote agent development.</p> <p>FY 2016 Plans: Will continue EMD for the NETT. NETT will be 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 will be 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. The Cyber domain will be the most rapidly changing domain in which our systems operate. The NETT program will research these new capabilities and will use an in-depth process to clean, fix, and integrate required Threat tools, tactics, and techniques that will be needed during T&E. Focus areas will include continued Threat integration, instrumentation, distributed collaboration, and remote agent development.</p>			
<p>Title: Threat Systems Management Office's (TSMO) Threat Operations</p> <p>Description: TSMO's Threat Operations program manages, maintains, and sustains a mission ready suite of threat systems within the Army's Threat inventory.</p> <p>FY 2014 Accomplishments: The Threat Operations program funded 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 edmultiple Army test events including (Network Integration Evaluation - NIE/Capabilities Integration Evaluation - CIE) and anticipated excursion test events for numerous Systems Under Test (SUT)/Programs of Record (POR) currently identified through FY16. FY14 funding</p>		2.868	2.838
			2.959

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015	
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0604256A / <i>Threat Simulator Development</i>	Project (Number/Name) 976 / <i>Army Threat Sim (ATS)</i>	
B. Accomplishments/Planned Programs (\$ in Millions)		FY 2014	FY 2015
<p>provided for acquisition life cycle management support and operation, maintenance, spares, new equipment training, special tools and instrumentation, additional DIACAP updates, etc, of new threat systems fielded into the Army's Threat inventory.</p> <p>FY 2015 Plans: The Threat Operations program funds 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 to support multiple Army test events including (Network Integration Evaluation - NIE/Capabilities Integration Evaluation - CIE) and anticipated excursion test events for numerous Systems Under Test (SUT)/Programs of Record (POR) currently identified through FY16. FY15 funding provides for acquisition life cycle management support and operation, maintenance, spares, new equipment training, special tools and instrumentation, additional DIACAP updates, etc, of new threat systems fielded into the Army's Threat inventory.</p> <p>FY 2016 Plans: The Threat Operations program 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 in order to support multiple Army test events including (Network Integration Evaluation - NIE/Army Warfighter Assessments - AWA) and anticipated excursion test events for numerous Systems Under Test (SUT)/Programs of Record (POR) currently identified through FY16.</p>			
<p>Title: Threat Intelligence and Electronic Warfare Environment (TIEW ENV).</p> <p>Description: Continues EMD for the TIEW ENV to simulate Electronic Warfare capabilities.</p> <p>FY 2014 Accomplishments: Continued EMD for the TIEW ENV: The TIEW ENV supported the establishment of a wrap-around threat environment required to evaluate, demonstrate, and employ the Electronic Warfare (EW) capabilities of Enemy Forces in simulated real-world test/training events. The TIEW ENV provided the capability to import vignettes, established virtual entities, connected live assets, and interacted between the live, virtual, and constructive environments. The TIEW ENV fully integrated with the ITF to enable Opposing Forces (OPFOR) command of threat EW assets across Live, Virtual, and Constructive (LVC) domains. FY14 satisfied Army requirements by funding development, platform integration and sustainment of this capability. Program fields incremental capabilities in support of upcoming spin out events. Additional capabilities included the initial development of Threat Directed Energy Weapons (TDEW) model (which include threat Radio Frequency (RF) weapon simulators and instrumentation that employs next generation RF weapon capabilities against US Army systems that rely on survivable and robust sensors for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance, continuous situational awareness, alert warning information and targeting) and continued integration with the ITF for robust LVC domain capability. The</p>		3.813	3.736
			-

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015	
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0604256A / <i>Threat Simulator Development</i>	Project (Number/Name) 976 / <i>Army Threat Sim (ATS)</i>	
B. Accomplishments/Planned Programs (\$ in Millions)		FY 2014	FY 2015
<p>TIEW ENV began the integration, via the ITF, with the live Directed Energy Weapon assets and the Threat Unmanned Device. Integration with the Network Exploitation Test Tool (NETT) also began in the latter part of FY14.</p> <p>FY 2015 Plans:</p> <p>Continues EMD for the TIEW ENV: The TIEW ENV supports the establishment of a wrap-around threat environment required to evaluate, demonstrate, and employ the Electronic Warfare (EW) capabilities of Enemy Forces in simulated real-world test/ training events. The TIEW ENV provides the capability to import vignettes, establish virtual entities, connect live assets, and interact between the live, virtual, and constructive environments. The TIEW ENV fully integrates with the Intergrated Threat Force (ITF) to enable Opposing Forces (OPFOR) command of threat EW assets across Live, Virtual, and Constructive (LVC) domains. FY15 satisfies Army requirements by funding development, platform integration and sustainment of this capability. Program fields incremental capabilities in support of upcoming spin out events. Continues development of Threat Directed Energy Weapons (TDEW) models as well as Intelligence, Surveillance, and Reconnaissance (ISR) & Camouflage, Concealment, Deception and Obscurants (CCD&O) models. In addition, the TIEW ENV will continue integration, via ITF, with the live Directed Energy Weapon assets, the Threat Unmanned Device and the Network Exploitation Test Tool (NETT).</p>			
<p>Title: Integrated Threat Force (ITF), formerly named Threat Battle Command Center (TBCC)</p> <p>Description: Continues the EMD phase for the ITF program to continue hardware/software development and threat systems integration in support to the build-out of the threat force architecture.</p> <p>FY 2014 Accomplishments:</p> <p>Completed the EMD phase for Increment 3 of the ITF program to enhance the ITF's Threat Battle Command applications, the Command, Control and Communicatons (C3) interfaced with the Increment 1 and 2 threat systems as well as completed the integration of the Camouflage, Concealment, Deception, and Obscurants (CCD&O) assets. FY14 delivered the final instrumentation capability for the ITF as well as completed the integration of the Command and Control (C2) functionality into the TBCC. FY14 funding fulfilled the Key Performance Parameters (KPPs) for Increment 3 while ensuring that the ITF program continued to meet the C3 and data fusion needs required to successfully meet scalability and reconfigurability needs for current Test & Evaluation (T&E) requirements.</p> <p>FY 2015 Plans:</p> <p>Initiates the EMD phase for Increment 4 of the ITF program to enhance the ITF's Threat Battle Command applications, the C3 interfaces with the Increment 1 - 3 threat systems as well as enhance the C2 functionality of the Threat Battle Command Center (TBCC). FY15 supports the initial design and development of distributed C2 functionality from the TBCC. Fulfills the KPPs for Increment 4 while ensuring that the ITF program will continue to meet the C3 and data fusion needs required to successfully meet scalability and reconfiguring needs for current T&E requirements.</p> <p>FY 2016 Plans:</p>		3.916	3.481
			3.823

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015		
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0604256A / Threat Simulator Development	Project (Number/Name) 976 / Army Threat Sim (ATS)		
B. Accomplishments/Planned Programs (\$ in Millions)		FY 2014	FY 2015	FY 2016
Will continue the EMD phase for Increment 4 of the ITF program to enhance the ITF's Threat Battle Command applications, the C3 interfaces with the Increment 1 - 3 threat systems as well as enhance the C2 functionality of the Threat Battle Command Center (TBCC). FY16 will support the initial design and development of distributed C2 functionality from the TBCC. Will fulfill the KPPs for Increment 4 while ensuring that the ITF program will continue to meet the C3 and data fusion needs required to successfully meet scalability and reconfiguring needs for current T&E requirements.				
Title: Threat Computer Network Operations Teams (TCNOT) Description: The TCNOT supports Army Test and Evaluation events by maintaining a team of highly qualified, trained, and certified Computer Network Operations (CNO) professionals who execute cyber operations against systems under test. The TCNOT program was designated a "Threat CNO Team" under AR 380-53 recognized as a USSTRATCOM/NSA certified "Red Team". FY 2014 Accomplishments: The Threat CNO Team program established and maintained 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 FY14 funded requirements to include continued research of the intelligence-based TCNO Techniques, Tactics and Procedures (TTP) 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. FY 2015 Plans: Funding supports unique training, credentials, and authorizations involving organizations such as Army 1st IO Command, NSA, HQDA-G2, and industry. FY15 funds requirements such as continued research of the intelligence-based TCNO TTP 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. FY 2016 Plans: Funding will support unique training, credentials, and authorizations involving organizations such as Army 1st IO Command, NSA, HQDA-G2, and industry. FY16 will fund requirements such as continued research of the intelligence-based TCNO TTP 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.		2.744	2.946	3.003
Title: Threat Computer Network Operations (CNO) Fidelity Enhancements		-	1.280	1.312

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015		
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0604256A / Threat Simulator Development	Project (Number/Name) 976 / Army Threat Sim (ATS)		
B. Accomplishments/Planned Programs (\$ in Millions)		FY 2014	FY 2015	FY 2016
<p>Description: Threat CNO Fidelity Enhancements is a new start project that will establish high-fidelity Threat malware and real-world tools, tactics, techniques, and procedures of Threat employment of CNO using commercial IT Technologies intended to engage complex U.S. operations.</p> <p>FY 2015 Plans: Program establishes validated high-fidelity Threat malware and real-world tools, tactics, techniques, and procedures of Threat employment of CNO using commercial IT technologies intended to engage complex U.S. operations. Develops state and non-state threat targeting packages that are "current", accurately profiling attack trends and timelines, intent, levels of sophistication, and threat training that will otherwise not be available to evaluate the exploitation of existing vulnerabilities in Enterprise Business Systems and network enabled systems. These threat packages range from "technological nomads" operating autonomously to state level forces using both active and passive network attack to selectively degrade or disrupt Army Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) and Enterprise Business Systems.</p> <p>FY 2016 Plans: Program will continue to validate high-fidelity Threat malware and real-world tools, tactics, techniques, and procedures of Threat employment of CNO using commercial IT technologies intended to engage complex U.S. operations. Will develop state and non-state threat targeting packages that are "current", accurately profiling attack trends and timelines, intent, levels of sophistication, and threat training that will not be available to evaluate the exploitation of existing vulnerabilities in Enterprise Business Systems and network enabled systems. These threat packages range from "technological nomads" operating autonomously to state level forces using both active and passive network attack to selectively degrade or disrupt Army C4ISR and Enterprise Business Systems.</p>				
<p>Title: Advanced Networked Electronic Support Threat Sensors (NESTS)</p> <p>Description: Program will begin prototype design and implementation to deliver advanced threat Electronic Support (ES) platforms.</p> <p>FY 2016 Plans: The Advanced NESTS program will increase existing threat Electronic Support (ES) capabilities to match the U.S. Intelligence Community performance assessments of real-world threat capabilities. This program seeks to replicate emerging real-world threat capabilities targeting advanced U.S. communication systems operating up to 18GHz. Program will establish the detailed design and begin the integration effort.</p>		-	-	2.392
<p>Title: Advanced Jammer Suite (Next Generation Electronic Attack (EA))</p>		-	-	1.758

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015	
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0604256A / <i>Threat Simulator Development</i>	Project (Number/Name) 976 / <i>Army Threat Sim (ATS)</i>	
B. Accomplishments/Planned Programs (\$ in Millions)		FY 2014	FY 2015
Description: Begin development of the infrastructure and testing capacity for persistent portrayal of operationally realistic threat network environments and expertise needed to accurately characterize, plan, and assess the effects of both US and adversary cyber capabilities. Enables ability to provide cyber attack capabilities from a realistic threat environment.			
FY 2016 Plans: The Advanced Jammer Suite expands the Army's open air and alternatives for EA in a test environment by using variations of jamming to include direct jamming, open air jamming and GPS jamming. This program will keep the current jamming threat as an asset to the Army for use in testing, at lower test costs. The Advanced Jammer Suite expands the Army alternative EA in a test environment by using appropriate jamming techniques for the applied testing environment. This program continues the threat representation for the Army in the jamming domain. This program will procure upgraded injection jamming units, as well as develop new and future jamming threats, to include satellite jamming threats. This threat development would include but is not limited to techniques such as Frequency Follower Direct Sequence Spread Spectrum (DSSS) threat jamming; Digital Radio Frequency Modulation (DRFM) "spoofing;" and, extended RF range into the Extremely High Frequency (EHF) range.			
Title: Threat Information Environment Description: Begin development of the infrastructure and testing capacity for persistent portrayal of operationally realistic threat network environments and expertise needed to accurately characterize, plan, and assess the effects of both US and adversary cyber capabilities. Enables ability to provide cyber attack capabilities from a realistic threat environment.		-	-
FY 2016 Plans: This capability will provide the infrastructure and testing capacity for routine and consistent portrayal of operationally realistic, threat representative environments and expertise and the means to accurately characterize, plan, and assess the effects of cyber adversaries. This program will leverage partnerships across the Army (ARCYBER/1st IO CMD, RDECOM/ARL, AMRDEC) to ensure intellectual capital and manning is available to execute the capability. Army cost avoidance through this program due to corrected vulnerabilities and threat mitigation in Army systems, would be both common and substantial.			1.000
Accomplishments/Planned Programs Subtotals		23.598	18.057
		FY 2014	FY 2015
Congressional Add: Integrated Threat Distributed Cyber Environments FY 2015 Plans: Development of these provisions will enable real-time cyber causality assessment against the realistic cyber threat environment while retaining the ability to rapidly reconfigure required environments as the cyber threat adapts and proliferates. This capability will utilize automated configuration and control of threat cyber environment operations in order to meet current demands. This capability is a solution to existing		-	4.000

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0604256A / <i>Threat Simulator Development</i>	Project (Number/Name) 976 / <i>Army Threat Sim (ATS)</i>

	FY 2014	FY 2015
challenges of implementing, sustaining, and reconfiguring actual foreign network technology to replicate threat cyber environment requirements.		
Congressional Adds Subtotals	-	4.000

C. Other Program Funding Summary (\$ in Millions)
 N/A

Remarks

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
 N/A