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

Date: March 2014

Appropriation/Budget Activity

R-1 Program Element (Number/Name)

2040: Research, Development, Test & Evaluation, Army I BA 6: RDT&E

PE 0604256A I THREAT SIMULATOR DEVELOPMENT

Management Support

COST (\$ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO <sup>#</sup>	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
Total Program Element	-	16.409	23.921	18.062	-	18.062	18.780	22.599	20.403	21.352	-	-
976: Army Threat Sim (ATS)	-	16.409	23.921	18.062	-	18.062	18.780	22.599	20.403	21.352	-	-

<sup>&</sup>lt;sup>#</sup> The FY 2015 OCO Request will be submitted at a later date.

#### Note

Army

FY13 adjustments attributed to Congressional General Reductions (-37 thousand); SBIR/STTR transfers (-244 thousand); and Sequestration reductions (-1.4 million).

### 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.

PE 0604256A: THREAT SIMULATOR DEVELOPMENT

UNCLASSIFIED
Page 1 of 9

Date: March 2014

Appropriation/Budget Activity

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

2040: Research, Development, Test & Evaluation, Army I BA 6: RDT&E

R-1 Program Element (Number/Name)
PE 0604256A / THREAT SIMULATOR DEVELOPMENT

Management Support

B. Program Change Summary (\$ in Millions)	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total
Previous President's Budget	18.090	16.934	19.180	-	19.180
Current President's Budget	16.409	23.921	18.062	-	18.062
Total Adjustments	-1.681	6.987	-1.118	-	-1.118
<ul> <li>Congressional General Reductions</li> </ul>	-0.037	-0.013			
<ul> <li>Congressional Directed Reductions</li> </ul>	-	-			
<ul> <li>Congressional Rescissions</li> </ul>	-	-			
<ul> <li>Congressional Adds</li> </ul>	-	7.000			
<ul> <li>Congressional Directed Transfers</li> </ul>	-	-			
<ul> <li>Reprogrammings</li> </ul>	-	-			
<ul> <li>SBIR/STTR Transfer</li> </ul>	-0.244	-			
<ul> <li>Adjustments to Budget Years</li> </ul>	-	_	-1.118	-	-1.118
Other Adjustments	-1.400	-	-	-	-

Exhibit R-2A, RDT&E Project Ju	ıstification	: PB 2015 A	rmy							Date: Marc	ch 2014	
Appropriation/Budget Activity 2040 / 6					` ` ` '				Project (Number/Name) 976 I Army Threat Sim (ATS)			
COST (\$ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO <sup>#</sup>	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
976: Army Threat Sim (ATS)	-	16.409	23.921	18.062	-	18.062	18.780	22.599	20.403	21.352	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

<sup>\*</sup> The FY 2015 OCO Request will be submitted at a later date.

#### Note

Army

Threat Computer Network Operations (CNO) Fidelity Enhancements is a new start 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 used in Army training, developmental tests, 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 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 2013	FY 2014	FY 2015
Title: Network Exploitation Test Tool (NETT).	3.461	10.580	3.781
Articles:	-	-	-
<b>Description:</b> Continues Engineering Manufacturing and Development (EMD) for the NETT as a comprehensive Computer Network Operations (CNO) tool.			
FY 2013 Accomplishments:			
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 provided 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			

PE 0604256A: THREAT SIMULATOR DEVELOPMENT

UNCLASSIFIED
Page 3 of 9

	UNCLASSIFIED					
Exhibit R-2A, RDT&E Project Justification: PB 2015 Army			Date: M	larch 2014		
Appropriation/Budget Activity 2040 / 6				lame) Sim (ATS)		
B. Accomplishments/Planned Programs (\$ in Millions, Article Q	uantities in Each)	F	Y 2013	FY 2014	FY 2015	
tactics of state and non-state Threat and is supported by a robust Cicapabilities are introduced daily to hacking community. The NETT pin-depth process to clean, fix, and integrate required Threat tools, ta funding supported the continuation of exploit development, continue advanced exploit research and tool integration required to support the	rogram researched these new capabilities and utilized a ctics, and techniques that are needed during T&E. FY13 s support to the NETT Users Group, and maintained page	n B ce with				
FY 2014 Plans: Continues EMD for the Network Exploitation Test Tool (NETT). NET tool, designed for T&E, to portray evolving hostile and malicious Thr integrated suite of open-source/open-method exploitation tools whic capabilities. NETT is used by Threat CNO teams to replicate the tac robust CNO development environment. The Cyber domain is the matter than the NETT program researches these new capabilities and uses an tools, tactics, and techniques that will be needed during T&E. Focus distributed collaboration, and remote agent development.	eat effects within the cyber domain. The program provion havill be integrated with robust reporting and instrumentactics of state and non-state Threat and is supported by a cost rapidly changing domain in which our systems operatin-depth process to clean, fix, and integrate required Threat and Integrate Reported Reporte	des an ation te.				
FY 2015 Plans: Will continue EMD for the Network Exploitation Test Tool (NETT). N (CNO) tool, designed for T&E, to portray evolving hostile and malicid will provide an integrated suite of open-source/open-method exploits instrumentation capabilities. NETT will be used by Threat CNO tear will be supported by a robust CNO development environment. The which our systems operate. The NETT program will research these and integrate required Threat tools, tactics, and techniques that will Threat integration, instrumentation, distributed collaboration, and rer Title: TSMO Threat Operations	ous Threat effects within the cyber domain. The programation tools which will be integrated with robust reporting and to replicate the tactics of state and non-state Threat a Cyber domain will be the most rapidly changing domain new capabilities and will use an in-depth process to clean be needed during T&E. Focus areas will include continuous	n and and in an, fix,	2.704	2.868	2.838	
	Ar	ticles:		-	-	
<b>Description:</b> Threat Systems Management Office's (TSMO) Threat mission ready suite of threat systems within the Army's Threat inven		а				
FY 2013 Accomplishments: Government Program Management for the TSMO Operations funde capability for Threat systems used to portray a realistic threat enviro Threat inventory. Included acquisition life cycle management support	nment during Army testing and training within the Army's	3				

PE 0604256A: THREAT SIMULATOR DEVELOPMENT

Army

UNCLASSIFIED Page 4 of 9

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army			Date: M	arch 2014	
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0604256A I THREAT SIMULATOR DEVELOPMENT  Project (Number/Name) 976 I Army Threat Sim (ATS)				
B. Accomplishments/Planned Programs (\$ in Millions, Article Quantit	ties in Each)		FY 2013	FY 2014	FY 2015
special tools and instrumentation, safety, environmental, security, informa the Army's Threat inventory. Funding supported the scheduled Life Cycle		into			
FY 2014 Plans: Continuing the Threat Operations program funds the operation, maintenar systems used to portray a realistic threat environment during Army testing to support multiple Army test events including (Network Integration Evalua anticipated excursion test events for numerous Systems Under Test (SUT FY16. FY14 funding provides for acquisition life cycle management supportraining, special tools and instrumentation, additional DIACAP updates, et inventory.	g and training within the Army's Threat inventory in ation - NIE/Capabilities Integration Evaluation - CIE )/Programs of Record (POR) currently identified the ort and operation, maintenance, spares, new equip	order E) and nrough oment			
FY 2015 Plans: Continuing the Threat Operations program will fund the operation, mainter Threat systems used to portray a realistic threat environment during Army in order to support multiple Army test events including (Network Integratio - CIE) and anticipated excursion test events for numerous Systems Under identified through FY16. FY15 funding will provide for acquisition life cycle spares, new equipment training, special tools and instrumentation, additio into the Army's Threat inventory.	v testing and training within the Army's Threat inversion Evaluation - NIE/Capabilities Integration Evaluat or Test (SUT)/Programs of Record (POR) currently e management support and operation, maintenance	ntory ion ce,			
Title: Threat Intelligence and Electronic Warfare Environment (TIEW ENV		rticles:	2.286	3.813	3.73
<b>Description:</b> Continues EMD for the Threat Intelligence and Electronic W Warfare capabilities.					
FY 2013 Accomplishments:  Continued EMD for the TIEW ENV: The TIEW ENV supports the establish to evaluate, demonstrate, and employ the EW capabilities of Enemy Force TIEW ENV provides the capability to import vignettes, establishes virtual the live, virtual, and constructive environments. The TIEW ENV fully integration and of threat EW assets across Live, Virtual, and Constructive (LVC funding development, platform integration and sustainment of this capabili upcoming spin out events.	es in simulated real-world test/training events. The entities, connects live assets, and interacts between grates with ITF to enable Opposing Forces (OPFO) domains. FY13 satisfied Army requirements by	en R)			
FY 2014 Plans:					

PE 0604256A: THREAT SIMULATOR DEVELOPMENT Army

UNCLASSIFIED Page 5 of 9

	UNCLASSIFIED				
Exhibit R-2A, RDT&E Project Justification: PB 2015 Army			Date: N	larch 2014	
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0604256A I THREAT SIMULATOR DEVELOPMENT		(Number/Number/Numy Threat		
B. Accomplishments/Planned Programs (\$ in Millions, Article Qu	uantities in Each)		FY 2013	FY 2014	FY 2015
Continues EMD for the TIEW ENV: The TIEW ENV supports the estate evaluate, demonstrate, and employ the Electronic Warfare (EW) capate events. The TIEW ENV provides the capability to import vignettes, we between the live, virtual, and constructive environments. The TIEW E (OPFOR) command of threat EW assets across Live, Virtual, and Co by funding development, platform integration and sustainment of this of upcoming spin out events. Additional capabilities include the initial model (which include threat Radio Frequency (RF) weapon simulator weapon capabilities against US Army systems that rely on survivable awareness, alert warning information and targeting) and continued in The TIEW ENV also begins the integration, via the ITF, with the live ID Device. Integration with the Network Exploitation Test Tool (NETT) as	abilities of Enemy Forces in simulated real-world text/tr vill establish virtual entities, connect live assets, and inte ENV fully integrates with the ITF to enable Opposing For instructive (LVC) domains. FY14 satisfies Army require capability. Program fields incremental capabilities in some development of Threat Directed Energy Weapons (TD res and instrumentation that employs next generation RF and robust sensors for C4ISR, continuous situational tegration with the ITF for robust LVC domain capability Directed Energy Weapon assets and the Threat Unmar	aining eract rces ments upport EW)			
FY 2015 Plans: Will continue EMD for the TIEW ENV: The TIEW ENV will support the required to evaluate, demonstrate, and employ the Electronic Warfard test/training events. The TIEW ENV will provide the capability to impand interact between the live, virtual, and constructive environments. Force (ITF) to enable Opposing Forces (OPFOR) command of threat domains. FY15 will satisfy Army requirements by funding development Program will field incremental capabilities in support of upcoming spir Energy Weapons (TDEW) models as well as Intelligence, Surveilland Deception and Obscurants (CCD&O) models. In addition, the TIEW Energy Weapon assets, the Threat Unmanned Device and the Network.	e (EW) capabilities of Enemy Forces in simulated real- fort vignettes, establish virtual entities, connect live assorate TIEW ENV will fully integrate with the Intergrated EW assets across Live, Virtual, and Constructive (LVC) Int, platform integration and sustainment of this capability on out events. Will continue development of Threat Direction, and Reconnaissance (ISR) & Camouflage, Concealing ENV will continue integration, via ITF, with the live Direction.	ets, Threat c) ty. cted ment,			
Title: Integrated Threat Force (ITF), formerly named Threat Battle Co			4.510	3.916	3.48
<b>Description:</b> Continues the EMD phase for the ITF program to continuintegration in support to the build-out of the threat force architecture.		rticles:	-	-	-
FY 2013 Accomplishments:  Continued EMD for the ITF which provides an integrated, scalable Threpresentations. This program leveraged prior Central Test & Evalua a highly adaptable and unique threat force capability to meet T&E recand SoS capabilities by closely simulating expected real-world threat	ation Investment Program (CEIP) investments to create quirements for the evaluation of network-centric platforr	n			

PE 0604256A: THREAT SIMULATOR DEVELOPMENT Army

UNCLASSIFIED Page 6 of 9

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army			Date: M	arch 2014	
Appropriation/Budget Activity 2040 / 6		t (Number/N Army Threat S	•		
B. Accomplishments/Planned Programs (\$ in Millions, Article	•	. [	FY 2013	FY 2014	FY 2015
hardware/software development/build-out supporting the threat for fusion needs required to successfully meet salability and reconfiguration.		, and			
FY 2014 Plans: Completes the EMD phase for Increment 3 of the ITF program to a C3 interfaces with the Increment 1 and 2 threat systems as well as Deception, and Obscurants (CCD&O) assets. FY14 also delivers completes the integration of the C2 functionality into the TBCC. FY (KPPs) for Increment 3 while ensuring that the ITF program will co successfully meet scalability and reconfigurability needs for current	s complete the integration of the Camouflage, Concealmer the final instrumentation capability for the ITF as well as Y14 funding is used to fulfill the Key Performance Parame entinue to meet the C3 and data fusion needs required to	nt,			
FY 2015 Plans: Will initiate the EMD phase for Increment 4 of the ITF program to einterfaces with the Increment 1 - 3 threat systems as well as enhar (TBCC). FY15 will support the initial design and development of d the Key Performance Parameters (KPPs) for Increment 4 while endata fusion needs required to successfully meet scalability and recommendation.	nce the C2 functionality of the Threat Battle Command Ce listributed C2 functionality from the TBCC. will be used to suring that the ITF program will continue to meet the C3 a	nter fulfill			
Title: Threat Computer Network Operations Teams (TCNOT)	Ar	ticles:	3.448	2.744	2.946
<b>Description:</b> The TCNOT supports Army Test and Evaluation ever certified Computer Network Operations (CNO) professionals who a TCNOT program was designated a "Threat CNO Team" under AR Team".	execute cyber operations against systems under test. The				
FY 2013 Accomplishments:  Continued the Threat CNO Team program in establishing and main professionals qualified for the employment of Threat CNO in support replicate the capabilities and hacker intent of state and non-state Tocould be exploited by Threat forces, replicating loss of service, or or create a desired effect. The funding supported unique training, as Army 1st IO Command, NSA, HQDA-G2, and industry. The FY intelligence-based TCNO Techniques, Tactics and Procedures (TI development of the necessary, highly specialized TCNO Training premerging foreign threat capabilities; and data collection capability.	ort of Army T&E. The Threat CNO Team mission is to accurate through identification of Army system vulnerabilities exploiting network enabled systems to gain critical informatoredentials, and authorizations involving organizations such 13 funded requirements to include continued research of TP) and threat portrayal capabilities up to the Nation State program; development, research, and analysis of continua	es that ation ch the level;			

PE 0604256A: THREAT SIMULATOR DEVELOPMENT Army

UNCLASSIFIED
Page 7 of 9

	UNCLASSIFIED				
Exhibit R-2A, RDT&E Project Justification: PB 2015 Army			Date: N	March 2014	
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0604256A I THREAT SIMULATOR DEVELOPMENT		ct (Number/l Army Threat		
B. Accomplishments/Planned Programs (\$ in Millions, Article (	Quantities in Each)		FY 2013	FY 2014	FY 2015
and correlate data of historical and real time malicious activity within DoD. This program also established services and near real-time propackages that accurately profile the cyber enemy, types of systems training, techniques, tools and operational tactics. The program reworking in concert with the Intelligence Community, capable of accorderational test requirements.	rocessing of information needed to develop threat targeting they attack, frequency of attacks, their intent, doctrine, sulted in creation of teams of Threat CNO professionals,	ng			
FY 2014 Plans: Continues the Threat CNO Team program in establishing and mair professionals qualified for the employment of Threat CNO in suppore plicate the capabilities and hacker intent of state and non-state the could be exploited by threat forces, replicating loss of service, or excreate a desired effect. The funding supports unique training, crede 1st IO Command, NSA, HQDA-G2, and industry. Funds requireme TCNO Techniques, Tactics and Procedures (TTP) and threat portrathe necessary, highly specialized TCNO Training program; develop threat capabilities; and data collection capability.	ort of Army T&E. The Threat CNO Team mission is to accordinate through identification of Army system vulnerabilitie exploiting network enabled systems to gain critical informatentials, and authorizations involving organizations such a not to include continued research of the intelligence-base ayal capabilities up to the Nation State level; development	s that tion or s Army d t of			
FY 2015 Plans: Will continue the Threat CNO Team program in establishing and m professionals qualified for the employment of Threat CNO in support to accurately replicate the capabilities and hacker intent of state an vulnerabilities that could be exploited by threat forces, replicating local critical information or create a desired effect. The funding will supporganizations such as Army 1st IO Command, NSA, HQDA-G2, an continued research of the intelligence-based TCNO Techniques, Taup to the Nation State level; development of the necessary, highly and analysis of continually emerging foreign threat capabilities; and	ort of Army T&E. The Threat CNO Team mission will be ad non-state threats through identification of Army system ass of service, or exploiting network enabled systems to gort unique training, credentials, and authorizations involving industry. The FY15 will fund requirements to include actics and Procedures (TTP) and threat portrayal capabil specialized TCNO Training program; development, research	jain ng ities			
Title: Threat Computer Network Operations (CNO) Fidelity Enhance	cements		-	-	1.280
<b>Description:</b> Threat CNO Fidelity Enhancements is a new start proworld tools, tactics, techniques, and procedures of Threat employmengage complex U.S. operations.					
FY 2015 Plans:					

PE 0604256A: THREAT SIMULATOR DEVELOPMENT Army

UNCLASSIFIED Page 8 of 9

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army			Date: March 2014
' ' '	,	, ,	umber/Name)

B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Program will establish 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. This program 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.			
Accomplishments/Planned Programs Subtotals	16.409	23.921	18.062

### 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 (SIRCM), 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

Army

PE 0604256A: THREAT SIMULATOR DEVELOPMENT

UNCLASSIFIED
Page 9 of 9