Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Army											Date: February 2016	
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 2015**	**FY 2016**	**FY 2017 Base**	**FY 2017 OCO**	**FY 2017 Total**	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**	**Cost To Complete**	**Total Cost**
Total Program Element	-	21.691	27.535	25.675	-	25.675	21.232	22.215	22.957	23.568	-	-
976: *Army Threat Sim (ATS)*	-	21.691	27.535	25.675	-	25.675	21.232	22.215	22.957	23.568	-	-

Note

Threat Battle Command Force (TBCF) is a new start in FY17. Integrated Threat Force (ITF) ends in FY17.

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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
Previous President's Budget	22.057	20.035	23.509	-	23.509
Current President's Budget	21.691	27.535	25.675	-	25.675
Total Adjustments	-0.366	7.500	2.166	-	2.166
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	7.500			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.366	-			
• Adjustments to Budget Years	-	-	2.166	-	2.166

Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Army	Date: February 2016
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army I* BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0604256A *I Threat Simulator Development*

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2015	FY 2016
Project: 976: *Army Threat Sim (ATS)*		
Congressional Add: *Integrated Threat Distributed Cyber Environments*	-	7.500
Congressional Add Subtotals for Project: 976	-	7.500
Congressional Add Totals for all Projects	-	7.500

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army			Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
976: *Army Threat Sim (ATS)*	-	21.691	27.535	25.675	-	25.675	21.232	22.215	22.957	23.568	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

Threat Battle Command Force (TBCF) is a new start in FY17. Integrated Threat Force (ITF) ends in FY17.

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 2015	FY 2016	FY 2017
Title: Network Exploitation Test Tool (NETT).	3.776	3.788	3.883
Description: Continues Engineering Manufacturing and Development (EMD) for the NETT as a comprehensive Computer Network Operations (CNO) tool. ***FY 2015 Accomplishments:*** Continued 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 issued 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 researched new capabilities and used an in-depth process to clean, fix, and integrate required Threat tools, tactics,			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
and techniques that were needed during T&E. Focus areas included continued Threat integration, instrumentation, distributed collaboration, and remote agent development. ***FY 2016 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 issued 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 to research new capabilities and to use an in-depth process to clean, fix, and integrate required Threat tools, tactics, and techniques that are needed during T&E. Focus areas to include continued Threat integration, instrumentation, distributed collaboration, and remote agent development. ***FY 2017 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 between multiple users, targets and attack visualization, data collection and remote agent development.			
Title: Threat Systems Management Office's (TSMO) Threat Operations ***Description:*** TSMO's Threat Operations program manages, maintains, and sustains a mission ready suite of threat systems within the Army's Threat inventory. ***FY 2015 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 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	6.472	2.959	3.395

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
training, special tools and instrumentation, additional DIACAP updates, etc, of new threat systems fielded into the Army's Threat inventory. ***FY 2016 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 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. ***FY 2017 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 FY17.			
Title: Threat Intelligence and Electronic Warfare Environment (TIEW ENV). ***Description:*** Completes EMD for the TIEW ENV to simulate Electronic Warfare capabilities. ***FY 2015 Accomplishments:*** Completes 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 funding will develop Intelligence, Surveillance, and Reconnaissance (ISR) & Camouflage, Concealment, Deception and Obscurants (CCD&O) models. In addition, FY15 funding will continue integration, via ITF, the Threat Unmanned Device and the Network Exploitation Test Tool (NETT). FY15 funding will complete this program.	3.736	-	-
Title: Integrated Threat Force (ITF), formerly named Threat Battle Command Center (TBCC) ***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. ***FY 2015 Accomplishments:***	3.481	3.823	1.965

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
Initiated the EMD phase for Increment 4 of the ITF program to enhance the ITF's Threat Battle Command applications, the Command, Control and Communications (C3) interfaces with the Increment 1 - 3 threat systems, as well as enhance the Command and Control (C2) functionality of the Threat Battle Command Center (TBCC). FY15 supports the initial design and development of distributed C2 functionality from the TBCC. ***FY 2016 Plans:*** Continues 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 continued design and development of distributed C2 functionality from the TBCC. ***FY 2017 Plans:*** 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). FY17 funding is expected to finish the design and development of distributed C2 functionality and fulfill the KPPs for Increment 4.			
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 and is accredited as a USSTRATCOM/NSA certified "Red Team". ***FY 2015 Accomplishments:*** Funded supports unique training, credentials, and authorizations involving organizations such as INSCOM, NSA, HQDA-G2, and industry. FY15 funded 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 supports unique training, credentials, and authorizations involving organizations such as INSCOM, NSA, HQDA-G2, and industry. FY16 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 2017 Plans:***	2.946	3.003	4.051

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
Funding will support unique training, credentials, and authorizations involving organizations such as INSCOM, NSA, HQDA-G2, and industry. FY17 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.			
Title: Threat Computer Network Operations (CNO) Fidelity Enhancements	1.280	1.312	1.333
Description: Threat CNO Fidelity Enhancements establishes 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. ***FY 2015 Accomplishments:*** Program established 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. Worked towards developing 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. ***FY 2016 Plans:*** Program continues 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. Continuing the development of 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. ***FY 2017 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 continue to 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			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
autonomously to state level forces using both active and passive network attack to selectively degrade or disrupt Army C4ISR and Enterprise Business Systems.			
Title: Advanced Networked Electronic Support Threat Sensors (NESTS) ***Description:*** Program will begin prototype design and implementation to deliver advanced threat Electronic Support (ES) platforms. ***FY 2016 Plans:*** The Advanced NESTS program to 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 to establish the detailed design and begin the integration effort. ***FY 2017 Plans:*** The Advanced NESTS program will continue to 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 continue the detailed design and the integration effort.	-	2.392	4.701
Title: Advanced Jammer Suite (Next Generation Electronic Attack (EA)) ***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. Program to 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. Program to 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. ***FY 2017 Plans:***	-	1.758	4.394

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
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 continue to 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 provides 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 would 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	-
Title: Threat Battle Command Force (TBCF) ***Description:*** Threat Battle Command Force (TBCF) ***FY 2017 Plans:*** The Threat Battle Command Force (TBCF) incorporates remote operations via distributed C2 while maintaining valid Threat tactics, techniques, and procedures (TTP) during T&E and training events. This program will integrate the Next Generation Electronic Support Suite, Next Generation Electronic Attack Suite and Computer Network Operations into future Threat C2 operations.	-	-	1.953
Accomplishments/Planned Programs Subtotals	21.691	20.035	25.675

	FY 2015	FY 2016
Congressional Add: Integrated Threat Distributed Cyber Environments	-	7.500

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 6	**R-1 Program Element (Number/Name)** PE 0604256A / *Threat Simulator Development*	**Project (Number/Name)** 976 / *Army Threat Sim (ATS)*

	FY 2015	FY 2016
FY 2016 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 challenges of implementing, sustaining, and reconfiguring actual foreign network technology to replicate threat cyber environment requirements.		
Congressional Adds Subtotals	-	7.500

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

N/A