Exhibit R-2, **RDT&E Budget Item Justification:** PB 2020 Army		**Date:** March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
Total Program Element	-	31.401	47.322	14.117	-	14.117	15.229	14.823	14.139	7.350	0.000	144.381
976: *Army Threat Sim (ATS)*	-	31.401	47.322	14.117	-	14.117	15.229	14.823	14.139	7.350	0.000	144.381

A. Mission Description and Budget Item Justification

This Program Element (PE) supports the design, development, acquisition, integration and fielding of realistic mobile threat simulators and realistic threat simulation products utilized in Army/Department of Defense (DoD) training and developmental and operational tests. This PE 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 United States (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 (SILs) and hardware/simulation in-the-loop facilities. These battlefield simulators represent adversary systems (e.g. missile systems, command, control and communications systems, electronic warfare systems, etc.) in order to portray a realistic threat environment during testing of U.S. weapon systems.

Army Threat Simulator and Threat Simulation products developed or fielded under this PE support Army-wide, non-system-specific threat product requirements. Each capability is pursued in concert and coordination with existing Army/DoD and Tri-Service capabilities to eliminate duplication of effort. 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 (DOT&E) Threat Simulator Investment Working Group.

B. Program Change Summary ($ in Millions)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
Previous President's Budget	22.862	12.835	15.284	-	15.284
Current President's Budget	31.401	47.322	14.117	-	14.117
Total Adjustments	8.539	34.487	-1.167	-	-1.167
• Congressional General Reductions	-0.009	-0.013			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	9.000	34.500			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.452	-			
• Adjustments to Budget Years	-	-	-1.167	-	-1.167

Exhibit R-2, **RDT&E Budget Item Justification:** PB 2020 Army	**Date:** March 2019
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*

Congressional Add Details ($ in Millions, and Includes General Reductions)	**FY 2018**	**FY 2019**
Project: 976: *Army Threat Sim (ATS)*		
Congressional Add: *Congressional Add: Integrated Threat Force*	9.000	-
Congressional Add: *Integrated Threat Force Cyber Threat Simulators*	-	6.000
Congressional Add: *Threat Cyberspace Operations*	-	10.000
Congressional Add: *Cyber Security Operations Center*	-	18.500
Congressional Add Subtotals for Project: 976	9.000	34.500
Congressional Add Totals for all Projects	9.000	34.500

Change Summary Explanation

Fiscal Year (FY) 2018 Congressional Add of $9.000 million for Integrated Threat Force.

FY19 Congressional Adds of $34.500 million for: Integrated Force Cyber Threat Simulators ($6.000 million); Threat Cyberspace Operations ($10.000 million); and Cyber Security Operations Center ($18.500 million).

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
976: *Army Threat Sim (ATS)*	-	31.401	47.322	14.117	-	14.117	15.229	14.823	14.139	7.350	0.000	144.381
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

In Fiscal Year 2020, management and oversight of Cyber Blue Team vulnerability assessments was moved from Project 976 to Program Element 0604759A (Major Test & Evaluation Investment), Project FF1 (Cyber Blue Team).

A. Mission Description and Budget Item Justification

This Project supports the design, development, acquisition, integration, and fielding of realistic mobile threat simulators and realistic threat simulation products utilized in Army/DOD training and developmental and operational tests. Army Threat Simulator and Threat Simulation products are utilized to populate test battlefields for United States (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 Project support Army-wide, non-system-specific threat product requirements. Each capability is pursued in concert and coordination with existing Army/DoD and Tri-Service capabilities to eliminate duplication of effort. 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 2018	FY 2019	FY 2020
Title: Network Exploitation Test Tool (NETT). ***Description:*** NETT is a comprehensive Threat Cyberspace Operations (TCO) tool designed for Test and Evaluation (T&E) to portray evolving hostile and malicious Threat effects within the Cyber domain. Program will continue to provide an integrated suite of open-source/open-method exploitation tools to be integrated with robust reporting and instrumentation capabilities. NETT is used by TCO teams to replicate the tactics of state and non-state Threats and is supported by a robust TCO development environment. The Cyber domain is the most rapidly changing domain in which our systems operate. NETT program will continue research of these capabilities and will use an in-depth process to clean, fix, sustain, modernize, and integrate required Threat tools, tactics, and techniques that will be needed during T&E. Focus areas include: continued Threat integration, instrumentation, distributed collaboration between multiple users, targets and attack visualization, data collection and remote agent development.	3.289	1.450	1.849

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
FY 2019 Plans: Continue EMD phase for the NETT including the integration of new tools, tactics, and techniques into the NETT to portray evolving Threat environments. ***FY 2020 Plans:*** Continue EMD phase for the NETT including the integration of new tools, tactics, and techniques into NETT in order to portray the evolving threat environment. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Minor adjustment in Army requirements.			
Title: Threat Systems Management Office's (TSMO) Threat Operations ***Description:*** 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/DoD test events including Network Integration Evaluation / Army Warfighting Assessment (NIE / AWA) and anticipated excursion test events for numerous Systems Under Test / Programs of Record (SUT / POR). ***FY 2019 Plans:*** Will continue to support multiple Army test events including NIE / AWA and anticipated excursion test events for numerous SUT / POR currently identified through FY2019. ***FY 2020 Plans:*** Will continue to support multiple Army test events including NIE / AWA and anticipated excursion test events for numerous SUT / POR currently identified through FY2020. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Minor adjustment in Army requirements.	3.552	1.256	1.429
Title: Threat Cyberspace Operations (TCO), formerly named Threat Computer Network Operations Team (TCNOT) ***Description:*** TCO supports Army/DoD events by maintaining a team of highly qualified, trained, and certified TCO professionals who execute Cyber operations against systems under test. The TCO program was designated a "Threat CNO Team" under Army Regulation (AR) 380-53 and is accredited as a United States Cyber Command (USCYBERCOM) / National Security Agency (NSA) certified "Red Team". ***FY 2019 Plans:***	5.764	0.565	2.444

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army			**Date:** March 2019
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 2018**	**FY 2019**	**FY 2020**
Funding provides for Contractor subject matter expertise within the Cyber Red Team workforce to support critical threat assessments. Beginning in FY2019, O&M funds will enable Cyber Red Team Department of the Army Civilian (DAC) subject matter expertise to execute this unique threat intelligence based mission (hence the reduction in FY2019 RDTE requirement). ***FY 2020 Plans:*** TCO funding provides for Contractor subject matter expertise within the Cyber Red Team workforce to support critical threat assessments. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Increased contract support in FY20 for critical threat assessments.			
Title: Threat Cyberspace Operations (TCO) Fidelity Enhancements. formerly named Threat Computer Network Operations (CNO) Fidelity Enhancements ***Description:*** Establishes high-fidelity Threat malware and real-world tools, tactics, techniques, and procedures of Threat employment of TCO using commercial Information Technologies (IT) intended to engage complex U.S. operations. Threat packages range from "technological nomads" operating autonomously to state level forces using both active and passive network attack to selectively degrade or disrupt C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) and Enterprise Business Systems. ***FY 2019 Plans:*** Program will continue the validation of high-fidelity threat malware and real-world tools, tactics, techniques, and procedures of threat TCO employment 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. These threat packages represent state and non-state level forces using both active and passive network attack to selectively degrade or disrupt Army C4ISR and Enterprise Business Systems. ***FY 2020 Plans:*** The TCO-FI program will continue the validation of high-fidelity threat malware and real-world tools, tactics, techniques, and procedures of threat TCO employment 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. These threat packages represent state and non-state level forces using both active and passive network attack to selectively degrade or disrupt C4ISR and Enterprise Business Systems. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Minor adjustment in Army requirements.	1.402	0.762	0.778
Title: Advanced Jammer Suite (AJS)	3.000	1.979	-

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army			**Date:** March 2019
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 2018**	**FY 2019**	**FY 2020**
Description: The Advanced Jammer Suite expanded the Army's open air and alternatives for Electronic Attack (EA) in a test environment by using variations of jamming to include direct jamming, open air jamming and GPS jamming. It kept the current jamming Threat as an asset to the Army for use in testing at lower test costs while expanding the Army alternative EA in a test environment by using appropriate jamming techniques for the applied testing environment. This program provided Threat representation for the Army/DoD in the jamming domain, developing new and future jamming threats, to include satellite jamming. ***FY 2019 Plans:*** Threat development will include, but is not limited to, techniques such as Frequency Follower Direct Sequence Spread Spectrum (DSSS) threat jamming; Digital Radio Frequency Memory (DRFM) "spoofing," and extended Radio Frequency (RF) range into the Extremely High Frequency (EHF) range. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** End of RDTE efforts for Advanced Jammer Suite in FY19.			
Title: Threat Battle Command Force (TBCF), formerly named Integrated Threat Force (ITF) ***Description:*** The Threat Battle Command Force (TBCF) incorporates remote operations via distributed Command and Control (C2) while maintaining valid Threat TTP during Tes & Evaluation (T&E) and training events. ***FY 2019 Plans:*** Integrate the Advanced Jammer Suite and additional Threat systems as identified by Threat assessments. Develop parsing tools to increase situational awareness for the Threat operations commander. Increase remote operations capabilities to decrease test costs. ***FY 2020 Plans:*** Integrate Advanced Electronic Support Sensor Suite (AESSS) initial capabilities and additional threat systems as identified by threat assessments. Increase on the move command and control capabilities to provide threat representative on the move capabilities to the threat operations commander. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** FY20 increase for Threat Battle Command Force (TBCF) for parsing tool development to increase situational awareness for the Threat Operations Commander, increase remote operations capabilities to decrease test costs and integrate the Advanced Electronic Support Sensor Suite (AESSS) capabilities to provide remote C2 capability network of unmanned sensors.	2.237	2.270	2.977
Title: Next Generation Mobile Communication Network Infrastructure Test Range (Next GEN MCNITR) ***Description:*** Next Generation MCNITR provides a mobile, scalable closed-loop cellular communications network infrastructure implementing multiple technologies capable of providing a realistic commercial Radio Frequency (RF) signals environment	0.657	1.166	2.003

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
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 2018**	**FY 2019**	**FY 2020**
needed for testing and training of U.S. forces in urban and suburban battle space environments. The Next Generation MCNITR program acquires a capability that simulates real-world RF signals environment and that supports representative Threat force reliance of network enabled devices dependent on advanced cellular technology. ***FY 2019 Plans:*** Integrate commercial RF technologies to create a threat faithful communications environment based upon results of the risk reduction phase. ***FY 2020 Plans:*** Continue development of 4GLTE IOC through Full Operational Capability (FOC). FOC will create threat representative commercial cellular environments. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** FY20 increase will be used to develop the 4GLTE FOC (IOC) baseline interoperable with Threat Battle Command Force creating threat representative commercial cellular environments.			
Title: Advanced Electronic Support Sensor Suite (AESSS) ***Description:*** AESSS provides expansion of Army's ability to portray acoustic, seismic, radio frequency, and electro-optical / infrared (EO/IR) sensor capabilities. ***FY 2019 Plans:*** Conduct risk reduction phase to decompose Threat requirements into system and sub-system functional requirements. ***FY 2020 Plans:*** Develop threat representative unmanned sensor mesh network leveraging lessons learned on prior programs. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** FY20 requirement represents expected cost of threat representative unmanned sensor mesh network development.	-	1.859	2.637
Title: Management and oversight of Cyber Blue Team vulnerability assessments ***Description:*** In 2016 the Army Acquisition Executive (AAE) designated PM ITTS as the Office of Primary Responsibility for Acquisition Blue Teams, to provide management and execution of relevant Cyber Blue Team assessment capabilities in support of the acquisition and test communities. Cyber Blue Teams refer to the cyber team which works cooperatively with the system owner to ensure programs can defend against attackers and/or Red Teams. These Cyber Blue Team capabilities are essential to enable military operators to assess and defeat the presence of cyber security threats across Army networks. PM ITTS will also serve as the primary point of contact for cyber-related testing and vulnerabilities assessments with U.S. Cyber Command and Army Cyber. This Project executes the establishment and management of certification standards for Acquisition Blue Teams	-	0.925	-

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
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 2018**	**FY 2019**	**FY 2020**
and coordination of Blue Team requirements on behalf of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA ALT). ***FY 2019 Plans:*** This activity will establish and manage certification standards for Cyber Blue Teams in coordination with all Project Managers on behalf of Assistant Secretary of the Army for Acquisition, Logistics, and Technology. It will be the single point of contact with United States Cyber Command (CYBERCOM) for open and closed networks, and will develop and field a central repository for vulnerability assessments. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Requirement is transferred to Program Element 0604759A (Major Test & Evaluation Investment) Project FF1 (Cyber Blue Team).			
Title: Advanced Networked Electronic Support Threat Sensors (NESTS) ***Description:*** In FY2018, Program began prototype design and implementation to deliver advanced threat Electronic Support (ES) platforms. The Advanced NESTS program aims to increase existing Threat ES capabilities to match U.S. Intelligence Community performance assessments of real-world Threat capabilities.	2.500	-	-
Title: FY19 SBIR/STTR Transfer ***Description:*** Small Business Innovation Research (SBIR) / Small Business Technology Transfer (STTR) ***FY 2019 Plans:*** Accounting for full funding amount. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Accounting for full funding amount.	-	0.590	-
Accomplishments/Planned Programs Subtotals	22.401	12.822	14.117

	FY 2018	**FY 2019**
Congressional Add: Congressional Add: Integrated Threat Force ***FY 2018 Accomplishments:*** Congressional Add: Integrated Threat Force	9.000	-
Congressional Add: Integrated Threat Force Cyber Threat Simulators ***FY 2019 Plans:*** Integrated Threat Force Cyber Threat Simulators	-	6.000
Congressional Add: Threat Cyberspace Operations	-	10.000

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
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 2018	FY 2019
FY 2019 Plans: Threat Cyberspace Operations		
Congressional Add: Cyber Security Operations Center ***FY 2019 Plans:*** Cyber Security Operations Center	-	18.500
Congressional Adds Subtotals	9.000	34.500

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

N/A