Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Army												Date: February 2020
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*							
COST ($ in Millions)	**Prior Years**	**FY 2019**	**FY 2020**	**FY 2021 Base**	**FY 2021 OCO**	**FY 2021 Total**	**FY 2022**	**FY 2023**	**FY 2024**	**FY 2025**	**Cost To Complete**	**Total Cost**
Total Program Element	-	46.732	42.117	14.515	-	14.515	14.807	14.125	7.343	11.236	0.000	150.875
976: *Army Threat Sim (ATS)*	-	46.732	42.117	14.515	-	14.515	14.807	14.125	7.343	11.236	0.000	150.875

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 2019**	**FY 2020**	**FY 2021 Base**	**FY 2021 OCO**	**FY 2021 Total**
Previous President's Budget	47.322	14.117	15.229	-	15.229
Current President's Budget	46.732	42.117	14.515	-	14.515
Total Adjustments	-0.590	28.000	-0.714	-	-0.714
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	28.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.590	-			
• Adjustments to Budget Years	-	-	-0.714	-	-0.714

Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Army	Date: February 2020
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 2019	FY 2020
Project: 976: *Army Threat Sim (ATS)*		
Congressional Add: *Integrated Threat Force Cyber Threat Simulators*	6.000	-
Congressional Add: *Threat Cyberspace Operations*	10.000	13.000
Congressional Add: *Cyber Security Operations Center*	18.500	15.000
Congressional Add Subtotals for Project: 976	34.500	28.000
Congressional Add Totals for all Projects	34.500	28.000

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
976: *Army Threat Sim (ATS)*	-	46.732	42.117	14.515	-	14.515	14.807	14.125	7.343	11.236	0.000	150.875
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

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/Department of Defense (DoD) training and developmental and operational tests. This 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 the 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 communication 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 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. 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 Cyber Test and Training (PM CT2) formerly Instrumentation, Targets and Threat Simulators (PM ITTS) and the Director, Operational Test and Evaluation (DOT&E) Threat Simulator Investment Working Group.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
Title: Network Exploitation Test Tool (NETT).	1.450	1.849	-
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.			
FY 2020 Plans:			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021
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 2020 to FY 2021 Increase/Decrease Statement:*** NETT will become part of Threat Information Warfare beginning FY2021.			
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 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 2020 to FY 2021 Increase/Decrease Statement:*** Threat Operations will become part of Threat Electronic Warfare beginning FY2021.	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 2020 Plans:*** TCO funding provides for Contractor subject matter expertise within the Cyber Red Team workforce to support critical threat assessments. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Threat Cyberspace Operations (TCO) will become part of Threat Information Warfare beginning FY2021.	0.565	2.444	-
Title: Threat Cyberspace Operations 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	0.762	0.778	-

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021
packages range from "technological nomads" operating autonomously to state level forces using both active and passive network attack to selectively degrade or disrupt 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 2020 to FY 2021 Increase/Decrease Statement:*** (TCO) Fidelity Enhancements will become part of Threat Information Warfare effort beginning FY2021.			
Title: Advanced Jammer Suite (AJS) ***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.	1.979	-	-
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 Test & Evaluation (T&E) and training events. ***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 2020 to FY 2021 Increase/Decrease Statement:*** Threat Battle Command Force (TBCF) will become part of Threat Network and Mission Command beginning FY2021.	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	1.166	2.003	-

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021
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 2020 Plans:*** Continue development of 4GLTE IOC through Full Operational Capability (FOC). FOC will create threat representative commercial cellular environments. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** (Next GEN MCNITR) will become part of Threat Network and Mission Command effort beginning FY2021.			
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 2020 Plans:*** Develop threat representative unmanned sensor mesh network leveraging lessons learned on prior programs. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** (AESSS) will become part of Threat Electronic Warfare effort beginning FY2021.	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 and coordination of Blue Team requirements on behalf of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA ALT).	0.925	-	-
Title: Threat Information Warfare ***Description:*** Provides cyber red team personnel and Information Operations (IO) weapons, Command and Control (C2), infrastructure, and research for advanced threat capabilities targeting Army programs, systems, and commands. Provides funds	-	-	5.334

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021
for cyber training and certifications of on-net interactive operators, certified ethical hackers, mission leads, planners and logistics. Access to real-time Internet flow information used for characterization of near-peer threats and the application of this information to Army targets. ***FY 2021 Plans:*** Identify mission sets with focus on the integration of Red Team operator capabilities into the Threat Environments mission set, i.e. provide not only integration of red assets but also include threat defense, threat blue teams, and general threat-based Cyber Network Defender (CND) operations. Operationalize (NETT) infrastructure and capabilities into a distributed cloud-based model such that other DoD Red Teams (joint teams) and Army teams can leverage the capability from geographically separated locations (fully distributed 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. 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. Development of threat targets and networks as new real-world targets sets and capabilities evolve. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Increased capability to meet evolving Army requirements with integration of (TCO), (NETT), and (TCO) Fidelity Enhancements			
Title: Threat Electronic Warfare ***Description:*** Develops Army threat Electronic Warfare capabilities that will simulate a realistic anti-access/aerial denial (A2/AD) environment that will portray critical threats to U.S. DoD satellite communication (SATCOM), navigation, and command, control, and communication (C3I) networks. Develops specific EW capabilities to include cyber/EW convergence, tailored jamming in a complex radio frequency (RF) environment, data spoofing, detection of Low Probability Intercept (LPI) waveforms, artificial intelligence (AI), network modeling, passive detection systems, and advanced electronic support systems. 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/ Department of Defense (DoD) test events including Joint Warfighting Assessment (JWA) and anticipated excursion test events for numerous Systems Under Test / Programs of Record (SUT / POR). ***FY 2021 Plans:*** Continue to develop and integrate electronic support sensors and electronic attack payloads to provide a robust and threat representative capability to support testing of Army systems. Threat Position, Navigation, and Timing (PNT) Jammer will consist of modifications and upgrades to ensure relevance by implementing additional capabilities within the PNT spectrum. Threat	-	-	4.177

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021
Operations will continue to support multiple Army test events including Joint Warfighting Assessment (JWA) and anticipated excursion test events for numerous Systems Under Test/ Programs of Record (SUT / POR) currently identified through FY2021. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Increase to Army requirements and addition of Electronic Support and Electronic Attack nodes and platforms.			
Title: Threat Network and Mission Command ***Description:*** Develops Army threat Network and Mission Command capabilities to include quantum computing techniques, use of adaptive RF transmissions, self-healing/mesh network, capabilities aimed at masking threat communication systems (Very High Frequency (VHF), Ultra High Frequency (UHF), and High Frequency (HF), satellite and cellular, and next generation tactical radios. ***FY 2021 Plans:*** Continue system integration and improve the network fidelity, as well as develop data fusion and artificial intelligence to provide improved decision aids to the Threat Force Commander. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Increased capability with integration of additional systems into the network.	-	-	5.004
Accomplishments/Planned Programs Subtotals	12.232	14.117	14.515

	FY 2019	FY 2020
Congressional Add: Integrated Threat Force Cyber Threat Simulators ***FY 2019 Accomplishments:*** Integrated Threat Force Cyber Threat Simulators	6.000	-
Congressional Add: Threat Cyberspace Operations ***FY 2019 Accomplishments:*** Threat Cyberspace Operations ***FY 2020 Plans:*** Threat Cyberspace Operations	10.000	13.000
Congressional Add: Cyber Security Operations Center ***FY 2019 Accomplishments:*** Cyber Security Operations Center ***FY 2020 Plans:*** Cyber Security Operations Center	18.500	15.000
Congressional Adds Subtotals	34.500	28.000

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 6	**R-1 Program Element (Number/Name)** PE 0604256A / *Threat Simulator Development*	**Project (Number/Name)** 976 / *Army Threat Sim (ATS)*

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A