Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Army												Date: May 2021
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 2020**	**FY 2021**	**FY 2022 Base**	**FY 2022 OCO**	**FY 2022 Total**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**Cost To Complete**	**Total Cost**
Total Program Element	-	41.566	41.486	18.439	-	18.439	-	-	-	-	-	-
976: *Army Threat Sim (ATS)*	-	41.566	41.486	18.439	-	18.439	-	-	-	-	-	-

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 for Simulation, Training and Instrumentation (PEO STRI) 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 Cyber Test and Training (PM CT2) and the Director, Operational Test and Evaluation (DOT&E) Threat Simulator Investment Working Group.

B. Program Change Summary ($ in Millions)	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Previous President's Budget	42.117	14.515	14.807	-	14.807
Current President's Budget	41.566	41.486	18.439	-	18.439
Total Adjustments	-0.551	26.971	3.632	-	3.632
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	27.500			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.551	-0.529			
• Adjustments to Budget Years	-	-	3.632	-	3.632

Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Army	Date: May 2021
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 2020	FY 2021
Project: 976: *Army Threat Sim (ATS)*		
Congressional Add: *Threat Cyberspace Operations*	13.000	3.750
Congressional Add: *Cyber Security Operations Center*	15.000	20.000
Congressional Add: *Cyber Threat Vunerabilities & Assessments*	-	3.750
Congressional Add Subtotals for Project: 976	28.000	27.500
Congressional Add Totals for all Projects	28.000	27.500

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army			Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
976: *Army Threat Sim (ATS)*	-	41.566	41.486	18.439	-	18.439	-	-	-	-	-	-
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 for Simulation, Training and Instrumentation (PEO STRI) 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) and the Director, Operational Test and Evaluation (DOT&E) Threat Simulator Investment Working Group.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Network Exploitation Test Tool (NETT).	1.699	-	-
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.			
Title: Threat Systems Management Office's (TSMO) Threat Operations	1.429	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
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).			
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".	1.773	-	-
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 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.	0.778	-	-
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.	3.097	-	-
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 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.	2.003	-	-
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.	2.787	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
Title: Threat Information Warfare	-	4.805	5.977
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 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 Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) and Enterprise Business Systems. Development of threat targets and networks as new real-world targets sets and capabilities evolve. ***FY 2022 Plans:*** Continue to 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 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 Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (C4ISR) and Enterprise Business Systems. Development of threat targets and networks as new real-world targets sets and capabilities evolve. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Increase aligns program requirements to Army Modernization priorities in support of the National Defense Strategy.			
Title: Threat Electronic Warfare	-	4.177	8.020
Description: Develops Army threat Electronic Warfare (EW) 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,			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
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 SUTs / PORs. ***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 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 2022 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 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 FY2022. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Army decreased funding in FY 2022 due to higher Army priorities.			
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 2022 Plans:***	-	5.004	4.442

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
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 2021 to FY 2022 Increase/Decrease Statement:*** Army decreased funding in FY2022 due to higher Army priorities.			
Accomplishments/Planned Programs Subtotals	13.566	13.986	18.439

	FY 2020	FY 2021
Congressional Add: Threat Cyberspace Operations ***FY 2020 Accomplishments:*** Supported Cyber Threat and vulnerability assessments through the enhancement of Cyber Threat simulators, including the research and development of cyber security solutions (tools, techniques, tactics & procedures). ***FY 2021 Plans:*** Support of Cyber Threat and vulnerability assessments through the enhancement of Cyber Threat simulators, including the research and development of cyber security solutions (tools, techniques, tactics & procedures).	13.000	3.750
Congressional Add: Cyber Security Operations Center ***FY 2020 Accomplishments:*** Support of Cyber Threat and vulnerability assessments to the Defense Industrial Base (DIB) through the enhancement of Cyber Threat representative tools and expertise, including the research and development of cyber security solutions (tools, techniques, tactics & procedures). ***FY 2021 Plans:*** Continue the Cyber Security Operations Center (CSOC) technical capabilities by engaging a variety of Defense Industrial Base (DIB) participants to conduct multiple prototype demonstrations. Continue gathering data to conduct the feasibility assessment of providing scalable cyber security expertise to the DIB. Develop and demonstrate the ability to provide secure real-time cyber support to a series of cloud enabled customer bases.	15.000	20.000
Congressional Add: Cyber Threat Vunerabilities & Assessments ***FY 2021 Plans:*** TSMO is chartered as the threat provider for the Army Acquisition community and provides Red Team capabilities to all branches of the DoD. As such, TSMO has a responsibility to continuously develop new and maintain existing threat capabilities, in the cyber, physical, intelligence, and EW domains. Cyber Vulnerability Assessments (CVA) allow TSMO to develop and test new capabilities in support of the Army Test and Evaluation, Cyber Operations Resiliency Assessment ? Platform (CORA-P), and Persistent Cyber Operation	-	3.750

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021
(PCO) missions. CVA will enable TSMO to more closely replicate advanced adversarial capabilities resulting in more threat faithful testing of critical Army weapon and information systems.		
Congressional Adds Subtotals	28.000	27.500

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A