Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Army	Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
Total Program Element	-	138.264	38.492	71.298	-	71.298	52.692	52.009	52.868	52.578	0.000	458.201
976: *Army Threat Sim (ATS)*	-	138.264	38.492	71.298	-	71.298	52.692	52.009	52.868	52.578	0.000	458.201

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) test and evaluation (T&E) 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.

This funding line supports testing of Army Modernization Priority Programs.

B. Program Change Summary ($ in Millions)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Previous President's Budget	138.937	38.492	33.544	-	33.544
Current President's Budget	138.264	38.492	71.298	-	71.298
Total Adjustments	-0.673	0.000	37.754	-	37.754
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.673	-			
• Adjustments to Budget Years	-	-	37.754	-	37.754

Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Army	Date: March 2024
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 2023	FY 2024
Project: 976: *Army Threat Sim (ATS)*		
Congressional Add: *Cyber Security Operations Center*	90.500	-
Congressional Add: *Supply Chain Illumination to Counter Emerging Threats*	5.000	-
Congressional Add: *Threat Counter Artificial Intelligence*	12.500	-
Congressional Add: *UAS Center of Excellence*	12.500	-
Congressional Add Subtotals for Project: 976	120.500	-
Congressional Add Totals for all Projects	120.500	-

Change Summary Explanation

The Army has identified significant shortfalls in Electronic Warfare (EW) and Information Warfare (IW) threat systems. The funding increase addresses the shortfall and will enable the Army to replicate an operationally realistic EW threat during test events.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army			Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
976: *Army Threat Sim (ATS)*	-	138.264	38.492	71.298	-	71.298	52.692	52.009	52.868	52.578	0.000	458.201
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) test and evaluation 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 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 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 and the Director, Operational Test and Evaluation Threat Simulator Investment Working Group.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: Threat Information Warfare	5.652	7.799	21.405
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 2024 Plans: Sustainment of existing threat-based Red Team capabilities, including previously developed toolsets and distributed operations infrastructure. Maintain Red Team Certification and Accreditation (C&A) required for on-network operations. Continued 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. These threat packages represent state and non-state level forces using			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
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 2023	FY 2024	FY 2025
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 2025 Plans:*** Development of existing threat-based Red Team capabilities, including previously developed toolsets and the Red Team Shared Infrastructure (RTSI) - a distributed operations infrastructure. Infrastructure hardware refresh. Maintain Red Team Certification and Accreditation required for on-network operations. Continued development of state and non-state threat targeting packages that are current, accurately profiling attack trends and timelines, intent, levels of sophistication, and threat test and evaluation. 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. Persistently replicates Advance Persistent Threats from near-peer actors across the materiel enterprise (into operations) which threaten Army modernization and readiness. Development of threat targets and networks as new real-world targets sets and capabilities evolve. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** FY 2024 to FY 2025 funding increase supports the development of higher fidelity Threat Information Warfare (TIW) capabilities in support of the increasing contested Information Operations (IO) domain. Increase also supports the replication of Advance Persistent Threats from near-peer actors across the materiel enterprise (into operations) which threaten Army modernization and readiness.			
Title: Threat Electronic Warfare ***Description:*** Develops Army Threat Electronic Warfare (EW) capabilities that will simulate a realistic anti-access/area 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 (air and ground), data spoofing, detection of Low Probability Intercept (LPI) waveforms, artificial intelligence (AI), network modeling, passive detection systems, and advanced electronic support systems such as Angle of Arrival (AoA) and Time Difference of Arrival (TDoA) against Low Probability of Detect (LPD) and Low Probability of Intercept (LPI) signals. Develops and prototypes Threat Electronic Support (ES) systems by leveraging state-of-the-art commercially available Software Defined Radio (SDR) technology incorporating Angle of Arrival (AoA), Time Difference of Arrival (TDoA), and/or Frequency Difference of arrival (FDoA) and integrates emerging processing techniques to include Machine Learning (ML) and Artificial Intelligence (AI). Provides a relevant and realistic threat battlespace environment inclusive of advanced ground and aerial sensor systems, low power ground surveillance systems, and other threat sensor systems employing non-RF applications (acoustic,	7.861	27.100	44.388

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
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 2023	FY 2024	FY 2025
seismic, and electro-optical/infrared). Integrates advanced sensor capabilities with existing threat Unmanned Aerial System (UAS) and threat command and control systems. Develops and prototypes Threat Electronic Attack (EA) systems by leveraging state-of-the-art commercially available SDR technology to develop jammers that function against numerous SUT operating on the full Radio Frequency (RF) spectrum. Provides jamming capabilities up to 40 GHz in order to target satellite uplinks, exploitable systems for Cyber & Electromagnetic Activities (CEMA), and a threat environment required for Multi-Domain Operations (MDO). Develops and prototypes a threat tactical communication replication effort that will leverage state-of-the-art commercially available SDR technology to present realistic signatures and Electronic Order of Battle (EOB) for the System Under Test (SUT). This system will cover threat tactical communication ranging from High Frequency (HF) to Super High Frequency (SHF). The Common Tactical Signal Emitter Program (CTSEP) will leverage intelligence community models to provide realistic, threat representative, signatures. Develops an affordable, common set of radar threat emitters based on commercial off-the-shelf (COTS) Software Defined Radios (SDR) technology to create a realistic RF signal dense threat environment for Multi-Domain Operations. Provides an affordable, common set of RF emitters needed to establish Tactical Communications and Gray-Space environments based on COTS SDR technology. Provides validated radar and communications digital models for use in a Live, Constructive, and Virtual environment as determined by Army Test & Evaluation Command (ATEC) to support Developmental Tests (DT) and Operational Tests (OT) for numerous Systems Under Test (SUT). ***FY 2024 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 Systems Management Office 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 FY 2024. ***FY 2025 Plans:*** Develop and integrate threat digital twin models, electronic support sensors and electronic attack payloads to provide a robust and threat representative capability to support testing of Army systems such as Terrestrial Layered System and Multi-Function Electronic Warfare System. Finalize development of Threat Position, Navigation, and Timing (PNT) Jamming environment, addressing needs for Army testing across the PNT spectrum. Continue development of Electronic Attack platforms, operating			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
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 2023	FY 2024	FY 2025
on the full Radio Frequency spectrum, ranging from the HF to UHF bands. Design, develop and integrate threat radar emitter systems to address radar shortfalls (VHF; UHF; Ku and Ka Bands). Provide jamming capabilities up to 40 GHz in order to target satellite uplinks, exploitable systems for Cyber & Electromagnetic Activities (CEMA), and a threat environment required for Multi-Domain Operations (MDO). Additionally, begin the development of threat representative tactical communication simulators that will leverage intelligence community models creating a realistic Multi-Domain Operations environment. The Army Threat Systems Management Office (TSMO) will continue to support multiple Army test events including Joint Warfighting Assessment and anticipated excursion test events for numerous Systems Under Test/ Programs of Record currently identified through FY2025. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** FY 2024 to FY 2025 funding increase provides Intelligence Community validated radar and communications digital models for use in a Live, Constructive and Virtual environment, as well as for rapid reprogramming of previously developed Software Defined Radio / Radar (SDR) open-air threat emitters that are required to be reactive to the threat. Additional funding will provide advanced jamming systems up towards 40 GHz (HF-Ka bands) in order to target satellite uplinks and expand the MDO environment to counter and test emerging system technologies that require an advanced frequency range. Additionally, increased funding will leverage COTS SDRs that ingest the intelligence community digital models to stimulate Systems Under Test (SUT) with threat realistic signatures.			
Title: Threat Network and Mission Command ***Description:*** Provides the Opposing Force (OPFOR) Commander and Staff with situational awareness of the Battlefield and Command, Control and Communications (C3) of threat systems across a dedicated communications network. 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 2024 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. 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). Threat Operations will continue to support multiple Army test events as well as procure new control systems to support future Multi Domain Operations. Development will continue with new system integrations and improve the network fidelity, as well as, develop data fusion and artificial intelligence to provide improved decision aids to the Threat Force	4.251	3.593	5.505

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
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 2023	FY 2024	FY 2025
Commander. 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. ***FY 2025 Plans:*** Continue system integration and improve the Threat Battle Command Force (TBCF) network fidelity to support the Threat Force Commander and aid in decision making. 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. Continue integration of the virtual and constructive threats coming from the eXpeditionary Live-virtual-constructive Command Center (XLCC) to enable live and simulated systems to interact and cause battlefield effects. Continue to improve threat cellular capabilities by upgrading to 5G technology in order to further enhance testing capabilities. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The increase in funding will ensure the development cycle for the program continues on track with previous scheduling for the development and integration of electronic support sensors, and the improvement of threat cellular capabilities.			
Accomplishments/Planned Programs Subtotals	17.764	38.492	71.298

	FY 2023	FY 2024
Congressional Add: Cyber Security Operations Center ***FY 2023 Accomplishments:*** FY 2023 Congressional Add Funding will provide prototype capability to evaluate the feasibility of providing cyber security services and expertise to the Defense Industrial Base (DIB). Provides for the development of techniques for providing on-site and remote DIB assistance with assessment, training, response, and mitigation of cyber vulnerabilities and industrial supply chains. Funding also develops and will demonstrate the ability to provide effective and secure real-time cyber support to a series of cloud-enabled distributed, or deployed government and/or industry customer bases.	90.500	-
Congressional Add: Supply Chain Illumination to Counter Emerging Threats ***FY 2023 Accomplishments:*** FY 2023 Congressional Add Funding provides the Supply Chain Illumination (WODEN Team) exhaustive illumination assessments of Army/DoD Program / Platform Supply Chains and associated reports for a combination of components and/or vendors. The Supply Chain team can assist the requesting agency with conducting Critical Function Analysis (CFA) on requested components or assess components to determine criticality and enhance overall horizontal protection against shared threats.	5.000	-
Congressional Add: Threat Counter Artificial Intelligence	12.500	-

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
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 2023	FY 2024
FY 2023 Accomplishments: FY 2023 Congressional Add Funding provides the capability for Threat Counter Artificial Intelligence (TCAI) to test emerging and evolving DOD/Army artificial intelligence (AI) and Machine Learning (ML) capabilities against operationally relevant and realistic threats.		
Congressional Add: UAS Center of Excellence ***FY 2023 Accomplishments:*** FY 2023 Congressional Add Funding provides the development of a UAS/ Counter UAS Center of Excellence including critical urban operating areas at the Redstone Test Center and Huntsville International Airport for the purpose of assessing UAS and Counter UAS detection, identification and mitigation technologies supporting DOD and DOJ. Capability also creates the premiere center to test and validate America's Counter UAS technologies charged with protecting critical infrastructure such as airports, power plants, dams, neighborhoods, etc. from drone incursions.	12.500	-
Congressional Adds Subtotals	120.500	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A