Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Army												Date: March 2023
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 2022**	**FY 2023**	**FY 2024 Base**	**FY 2024 OCO**	**FY 2024 Total**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**Cost To Complete**	**Total Cost**
Total Program Element	-	60.749	138.937	38.492	-	38.492	33.544	14.199	11.732	11.859	0.000	309.512
976: *Army Threat Sim (ATS)*	-	60.749	138.937	38.492	-	38.492	33.544	14.199	11.732	11.859	0.000	309.512

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.

This funding line supports testing of Army Modernization Priority Programs.

B. Program Change Summary ($ in Millions)	FY 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total
Previous President's Budget	61.422	18.437	11.581	-	11.581
Current President's Budget	60.749	138.937	38.492	-	38.492
Total Adjustments	-0.673	120.500	26.911	-	26.911
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	120.500			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-0.673	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	26.911	-	26.911

Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Army	Date: March 2023
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 2022	FY 2023
Project: 976: *Army Threat Sim (ATS)*		
Congressional Add: *Threat Cyberspace Operations*	3.000	-
Congressional Add: *Cyber Security Operations Center*	40.000	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	43.000	120.500
Congressional Add Totals for all Projects	43.000	120.500

Change Summary Explanation

Increase in FY 2024 funding is for the Multi-Domain Operation (MDO) driven threats and targets investments are critical in enabling a MDO contested and realistic Future Operating Environment for critical Operational Test events across the FYDP. A detailed threat gap analysis identified critical shortfalls in MDO threat capabilities and ensured alignment with Army G2 threat assessments.

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
976: *Army Threat Sim (ATS)*	-	60.749	138.937	38.492	-	38.492	33.544	14.199	11.732	11.859	0.000	309.512
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 2022	FY 2023	FY 2024
Title: Threat Information Warfare	5.683	5.601	7.799
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 2023 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 Cyber Network Defense (CND) operations. Expand Network Exploitation Test Tool (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			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024
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 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 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 2023 to FY 2024 Increase/Decrease Statement:*** Increase in funding for the Multi-Domain Operation (MDO) driven threats and targets investments are critical in enabling a MDO contested and realistic Future Operating Environment for critical Operational Test events across the FYDP. A detailed threat gap analysis identified critical shortfalls in MDO threat capabilities and ensured alignment with Army G2 threat assessments.			
Title: Threat Electronic Warfare ***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, 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), Cognitive RF processing techniques against Low Probability of Detect (LPD) and Low Probability of Intercept (LPI) signals. 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 (SUT)/ Programs of Record (POR).	7.711	8.136	27.100

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024
Develops and prototypes threat Electronic System (ES) by leveraging state-of-the-art commercially available Software Defined Radio (SDR) technology incorporating Angle of Arrival (AoA) and Time Difference of Arrival (TDoA) and Cognitive RF processing techniques against Low Probability of Detect (LPD) and Low Probability of Intercept (LPI) signals. ***FY 2023 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 2023. ***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 2023 to FY 2024 Increase/Decrease Statement:*** Increase in funding for the Multi-Domain Operation (MDO) driven threats and targets investments are critical in enabling a MDO contested and realistic Future Operating Environment for critical Operational Test events across the FYDP. A detailed threat gap analysis identified critical shortfalls in MDO threat capabilities and ensured alignment with Army G2 threat assessments. The increase in funding will provide a robust threat representative PNT enterprise within the Army to fully evaluate the susceptibility of US "Blue Force" PNT/Alternate Navigation systems against current and emerging denial and deception capabilities and techniques. Funding provides the ability to immerse Artificial Intelligence/Machine Learning-enabled blue force systems in an operationally relevant MDO test environment and perform actions that emulate real-world threats to those systems.			
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.	4.355	4.027	3.593

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024
FY 2023 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) currently identified through FY2023. ***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 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 2023 to FY 2024 Increase/Decrease Statement:*** Decrease in funding due to higher Army priorities.			
Title: SBIR/STTR Transfer ***FY 2023 Plans:*** Funding transferred in accordance with Title 15 USC §638 ***FY 2023 to FY 2024 Increase/Decrease Statement:*** Funding transferred in accordance with Title 15 USC §638	-	0.673	-
Accomplishments/Planned Programs Subtotals	17.749	18.437	38.492

	FY 2022	FY 2023
Congressional Add: Threat Cyberspace Operations	3.000	-

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023
FY 2022 Accomplishments: Support to 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). Provided cyber red team Information Operations (IO) weapons, Command and Control (C2) infrastructure, and research for advanced threat capabilities targeting Army programs, systems, and commands. Furthered efforts executed under FY21 185 $3,750K Program Increase "Threat Simulator Development"		
Congressional Add: Cyber Security Operations Center ***FY 2022 Accomplishments:*** Prototype capability evaluated the feasibility of providing cyber security services and expertise to the Defense Industrial Base (DIB). Refined techniques for providing on-site and remote DIB assistance with assessment, training, response, and mitigation of cyber vulnerabilities and industrial supply chains. Continued development and refinement of 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. The FY 2022 Congressional Add funds significantly increased the scale of support into the next phase of the prototype, which includes a drastically larger magnitude of DIB participants than executed in previous phases. ***FY 2023 Plans:*** 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.	40.000	90.500
Congressional Add: Supply Chain Illumination to Counter Emerging Threats ***FY 2023 Plans:*** Congressional Add FY2023 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 2024 Army		Date: March 2023
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 2022	FY 2023
FY 2023 Plans: FY2023 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	-	12.500
FY 2023 Plans: Congressional Add FY2023 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.		
Congressional Adds Subtotals	43.000	120.500

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A